Ministry
of Justice

Cyber Security Guidance

General Edition

Contents

Cyber and Technical Security Guidance

Summary

This site lists the https://www.gov.uk/government/organisations/ministry-of-justice Information Security policies. It contains important guidance on how to keep information safe and secure.

Policies shown here are listed for technical users and non-technical users (referred to as all users).

Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

The Technical Guidance covers technical decisions in the more widely.

Note: This guidance is dated: 8 November 2023.

Change log

A 'change log' is available. It details the most recent changes to this information.

The changes are also available as RSS or Atom feeds.

Searching this content

The security guidance is searchable in two ways:

1. By searching for the word or phrase on your preferred search engine, and specifying this site:

   ```
   site:https://security-guidance.service.justice.gov.uk/
   ```

   For example, to search for information about passwords, you might use the following search expression:

   ```
   password site:https://security-guidance.service.justice.gov.uk/
   ```
2. By downloading one of the offline versions and using the inbuilt search capability of your offline reader.

Offline content

This offline version of the guidance is available as a PDF file for convenience. However, it is time-limited: it is not valid after 8 December 2023. For the latest, current version of the guidance, refer to the security guidance site.

Security culture

In addition to the obvious security resources such as policies, controls, and software and hardware tools, all organisations need employees, suppliers and other colleagues to behave in a way that helps ensure good security at all times. A simple example is where someone will act in a way that maintains good security, even if they don't know exactly what the formal process is. The extent to which an organisation has good security in indicated by its security culture.

Security culture refers to the set of values, shared by everyone in an organisation, that determines how people are expected to think about and approach security. Getting security culture right helps develop a security conscious workforce, and promotes the desired security behaviours expected from everyone working in or for the organisation.

The is creating a portfolio of security culture resources to help supplement the formal policy and guidance material. Initial security culture material is available for preview.

Information structure

policy documents are listed beneath the following headings:

- Information security policies
- Mobile devices and teleworking
- Human resource security
- Asset management
- Access control
- Physical and environmental security
- Operations security
- Communications security
- Information security incident management
- Compliance
- Risk Assessment

The documents are listed in the next section.

Information security policies

Management direction for information security

These are the policies for all users:

- Avoiding too much security
- IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
- IT Security All Users Policy
- IT Security Policy (Overview)
- Line Manager approval

Mobile devices and teleworking

Mobile device policy

These policies are for all users:

- Mobile Device and Remote Working Policy
- Remote Working

Teleworking

This policy is for all users:

- Personal Devices

Human resource security

Prior to employment

This policy is for all users:

- Minimum User Clearance Levels Guide

During employment

This policy is for all users:

- Training and Education

Termination and change of employment

This policy is for all users:

- End or change of employment

Asset management

Responsibility for assets

These policies are for all users:

- Acceptable use
- Acceptable use policy
- Guidance on IT Accounts and Assets for Long Term Leave
- Protect Yourself Online
- Web browsing security

Information classification

These policies are for all users:

- Government Classification Scheme
- Information Classification and Handling Guide
- Information Classification and Handling Policy

Media handling

These policies are for all users:

- Removable media
- Secure disposal of IT equipment
- Secure disposal of IT - physical and on-premise
- Working securely with paper documents and files

Access control

User responsibilities

This policy is for all users:

- Protecting Social Media Accounts

Physical and environmental security

Equipment

These policies are for all users:

- Clear Screen and Desk Policy
- Equipment Reassignment Guide
- Laptops
- Locking and shutdown
- Policies for MacBook Users

Operations security

Protection from malware

This policy is for all users:

- Ransomware

Control of operational software

This policy is for all users:

- Guidance for using Open Internet Tools

Communications security

Information transfer

These policies are for all users:

- Bluetooth
- Email
- General Apps Guidance
- Phishing Guide
- Protecting WhatsApp accounts
- Secure Data Transfer Guide
- Sending information securely
- Web browsing security policy profiles
- Wifi security policy

Information security incident management

Management of information security incidents

These policies are for all users:

- IT Security Incident Management Policy
- IT Security Incident Response Plan and Process Guide
- Lost devices or other IT security incidents
- Reporting an incident

Compliance

Compliance with legal and contractual requirements

This policy is for all users:

- Data Security and Privacy

Risk Assessment

Risk Assessment Process

This policy is for all users:

- Risk reviews

Other Guidance

The provides the base material for all security guidance in the .

Glossary

A glossary of some terms used in this guidance is available here.

Acronyms

Technical Guidance

The Technical Guidance should be read together with this security-focused guidance.

Change log for Security Guidance

This document summarises what changes were made, and when, to Security policy and guidance. The most recent changes appear at the beginning of the list.

2023-09-11 17:45 BST Update ITHC details	Updates to information about IT Health Checks.
2023-08-30 17:45 BST Clearance requirements	Added details about minimum user clearance requirements.
2023-08-09 17:35 BST Build tooling updates	Updates to build tooling for security and performance improvements.
2023-07-13 17:00 BST Accessing MoJ IT systems from overseas	Removed topic on accessing MoJ IT systems from overseas.
2023-07-07 16:45 BST Taking equipment overseas	Removed general advice topic on taking equipment overseas.
2023-06-22 17:35 BST Formatting and terminology updates	Minor improvements to formatting, and updates to terminology.
2023-06-05 18:13 BST Updates to incident management policy	Refresh and add extra detail about managing security incidents.
2023-04-29 13:54 BST Add 1Password guidance	Add information about using the 1Password tool.
2023-04-18 17:10 BST Revise content	Updates to personnel and related information.
2023-03-21 17:35 GMT Restructure landing page, and added service owners responsibilities guidance	New material on service owner responsibilities.
2023-02-28 17:35 GMT Corrected policy reference number	Policy number POL.ITAUP.022 in the Acceptable Use Policy was incorrectly listed as number 021.
2023-02-16 17:35 GMT Corrected typo in template	Fixed minor typo in Asset template.
2023-02-08 17:35 GMT Updated remote working guidance	Clarification on using hotel or other public wifi spots.
2023-01-22 17:41 GMT Updated authorisation information	More details on implementing defensive depth and dealing with external IP addresses.
2023-01-10 18:04 GMT Updated contact details for secure disposal	When seeking help for secure disposal, contact IT Service Desk in the first instance.
2022-10-19 14:34 BST Updated project README	An update to the README and refresh of the content.
2022-08-31 09:50 BST Overseas travel	Clarification regarding transit or destination locations.
2022-08-30 10:43 BST Added guidance on protecting WhatsApp accounts	Extra information on how WhatsApp accounts might be attacked, and how to protect your accounts.

2022-08-09 12:17 BST Remove links to download leaflets

Remove links to leaflet downloads, ready for later updates.

2022-08-05 12:08 BST Add guidance on video conferencing hardware

Provide more details on the use of dedicated hardware for video and conference calls.

2022-08-04 16:22 BST Add connected vehicle reference in bluetooth guidance

Connected vehicles are discussed in personal devices, but the information also applies in the bluetooth guidance.

2022-07-22 13:14 BST Use of personal devices to receive MFA codes

Added clarification that personal devices may be used to receive MFA authentication codes if an MoJ-issued device is not available.

2022-07-21 13:45 BST Guidance on use of personal devices

Added clarification and emphasis that personal devices must not be used for work purposes. This includes accessing MoJ Slack channels using personal devices.

2022-07-04 14:23 BST Correct broken links

Internal links on a page were broken; now fixed.

2022-06-23 12:02 BST Accessibility updates

Improved the content tagging following guidance on accessibility improvements. Affects all pages, the link in this notification is to an example page.

2022-06-01 13:36 BST Reporting phishing

Clarified process for reporting phishing attempts.

2022-05-27 16:09 BST Add IASME certification information and templates.

Added material to assist suppliers in seeking security certification, particularly regarding the IASME Governance standard.

2022-05-20 15:37 BST Updates to overseas travel information.

More information about applying with sufficient advance notice, and a reminder about passport validity dates.

2022-05-06 12:30 BST Minor restructure to Phishing information.

The section on Out Of Band Checks has been slightly reordered, to improve readability.

2022-05-06 12:18 BST Added link to Password Poster.

An information poster about how to make strong passwords is now available for download.

2022-04-19 17:45 BST Update links for contacting security team.

Standardise on security@justice.gov.uk email address for contacting security team.

2022-04-08 10:09 BST Add guidance on secure disposal of cloud materials.

New guidance to ensure the confidentiality of MoJ data remains when a cloud service is decommissioned.

2022-04-06 15:53 BST Update security.txt link.

Corrected link to the standard security.txt file.

2022-04-04 10:50 BST Add password manager guidance.

Added extra information on the use of password manager apps in the MoJ.

2022-03-21 10:35 GMT Add guidance on sharing information.

Added extra information on sharing information internally and externally.

2022-03-21 10:22 GMT Add guidance on QR codes.

Added information on QR codes; currently considered low risk.

2022-03-11 15:31 GMT Updates to ransomware information leaflet.

Updates to correct typos and improve style.

2022-03-10 17:01 GMT Updates to LastPass guidance.

More information about when and how LastPass may be used.

2022-03-10 13:09 GMT Various minor corrections.

Fixing broken links and updating references to standards.

2022-03-04 09:16 GMT Updated email security guide.

Clarification that phishing or spoofing of MoJ colleagues, by MoJ colleagues, is not permitted other

	than with formal approval in advance, justified by a good business case.
2022-02-18 18:35 GMT Added phishing guide.	New topic, providing advice on dealing with phishing threats.
2022-02-16 11:19 GMT Updated security.txt file.	Provided new expiry date for security.txt file.
2022-02-15 12:18 GMT Various minor corrections.	Corrected contact details, fixed an incorrect link, and updated secure disposal information.
2022-02-07 15:49 GMT Updated glossary.	Expanded list of glossary definitions, and explanation of out-of-band-checks.
2022-02-01 11:51 GMT Update to passwords guidance.	A reminder not to share passwords or other account details.
2022-01-25 10:37 GMT Publication of ransomware information leaflet.	Useful leaflet explaining what Ransomware is, and tips on protecting your work and your systems.
2022-01-18 17:06 GMT Updated guidance for hosting platforms.	Updated baseline guidance for AWS and Azure platforms.
2022-01-07 14:36 GMT Contact details for AWS	Updated contact details for Baseline AWS accounts.
2022-01-06 09:36 GMT System lockdown and hardening	Guidance added to prevent outbound connections to random internet systems, unless this is a core part of their design. Firewall rules and other network configuration must prevent this.
2022-01-04 16:27 GMT IT Health Check	Updated guidance with a new section on Cloud platforms.
2022-01-04 16:10 GMT Update Slack channel for privacy team	Provide revised channel details for contact privacy team through Slack IM.
2021-12-23 13:50 GMT Update overseas travel guidance	Updates to information on overseas travel and accessing MoJ IT systems from overseas.
2021-12-21 13:18 GMT Provide seasonal SMS scam advice	Material to help improve awareness and best practices for security.
2021-12-15 15:09 GMT Use DuckDuckGo search engine	Default to using DDG for content search.
2021-12-13 11:44 GMT Security threat level guidance	New security threat Level guidance, and associated procedures.
2021-12-13 11:27 GMT Debrief on return from travel	Added description of a security debrief that is mandatory after some travel or where other security conditions apply.
2021-12-13 11:24 GMT Accessing MoJ systems from overseas	Added link to supplementary information on the MoJ Intranet.
2021-12-08 09:15 GMT Email access	Added clarification regarding when access is permitted to a user's business email account.
2021-12-07 15:18 GMT Email Authentication	Added guidance requiring the use of MTA-SLS and TLS-RPT in MoJ email systems.
2021-11-30 13:54 GMT Personal Devices	Clarified guidance on connecting personal devices using Bluetooth, and added new section on connected vehicles.

2021-11-22 16:23 GMT MFA	Clarified guidance on sending one-time MFA codes only to individual devices or accounts, not to shared devices or accounts.
2021-11-22 14:14 GMT Government Classification Scheme	Updated and consolidated guidance on classification of Government information.
2021-11-19 15:22 GMT Other guidance and security.txt	Improved structure for other guidance information, and added security.txt file.
2021-11-19 10:09 GMT Sending information securely	Guidance on working securely with paper documents and files.
2021-11-17 17:07 GMT Personal devices	Updated guidance about using a personal device to connect to a business Teams meeting as a Guest.
2021-11-09 15:37 GMT Acceptable use policy	Provide more detail on monitoring of systems and information, and to clarify the situation regarding Data Protection and the storage or processing of information outside the UK.
2021-11-08 17:30 GMT System backup policy	Corrected broken links within the content, also some structural changes for easier cross-referencing with related topics.
2021-11-04 09:05 GMT Working securely with paper documents and files	This guidance helps you understand the risks involved in working with, sharing, and moving paper documents both inside and outside the office.
2021-11-03 17:12 GMT Email blocking	The policy and processes for blocking emails, and deleting emails through administrative processes, across email services across the MoJ.
2021-11-03 17:00 GMT Domain names	An overview of domain name registration and monitoring principles and responsibilities within the MoJ.
2021-10-29 11:52 BST Logging retention	Information about keeping logging information.
2021-10-19 13:06 BST Remote working	Simplified the guidance regarding remote working.
2021-10-15 16:27 BST Email best practices	Added guidance regarding attachments and the use of 'cc' and 'bcc' fields in emails.
2021-10-14 13:47 BST Azure subscription baselines	Added guidance on baselines and templates for Azure subscriptions.
2021-10-13 15:50 BST IT Health Checks	Added guidance on requesting and managing IT Health Checks.
2021-10-08 09:56 BST Wifi policy	Added policy information about wifi.
2021-10-05 14:28 BST Client certificates	Added notes about obtaining client certificates.
2021-10-01 15:24 BST Connection to public wifi	Clarification about connecting to public wifi spots, such as hotels or coffee shops, or home broadband. Also extra details for remote working securely.
2021-10-01 15:07 BST Personal device attachment	Clarifying the connection of personal peripherals, and the charging of personal devices from USB ports.
2021-09-13 17:21 BST Government Security Standard 007 V2	Updates following the release of V2 of the Gov007 security standard.
2021-09-02 15:16:00 BST Extra guidance on remote working.	Additional best practices for keeping safe and secure when working away from the office.

2021-08-20 14:14:00 BST Update to general apps guidance.	Add Trello guidance, and clarification over Official and Official Sensitive material in apps.
2021-08-18 15:17:00 BST Add change log page.	Created a change log page, and associated RSS and Atom feeds, to describe new or changed content.
2021-08-16 17:04:00 BST Clarification for accessing MoJ IT systems overseas.	Additional information describing the process.
2021-08-16 17:03:00 BST Data Movement Form updated.	Data Movement Form updated.

Getting in contact

Reporting an incident

colleagues should visit https://intranet.justice.gov.uk/guidance/security/report-a-security-incident/ on the Intranet.

Security Team: asking for help

Overview

This document tells you about the Security Team. It explains how to ask for help, outlines how we handle your requests, and describes what happens next.

To ask for help from a security consultant, send an email to: .

About the team

The Security Team is part of Security & Privacy. The Chief Information Security Officer leads the team.

The team provides help and guidance around cyber security matters, such as:

- Understanding the risks facing your systems and services.
- Designing and implementing effective mitigations for these risks.
- Developing services using security best practices.
- Checking that you or your third party suppliers have enough, and appropriate, cyber security measures in place.
- Applying IT Security policy to specific scenarios.

Asking for help

If you need help dealing with a cyber security task or problem, send an email to:

Some requests are better handled by other teams. For urgent matters such as incidents, or to get help about physical or personnel security, contact . For help with data protection, contact .

The security team keep an eye open for email requests. Normally, you'll get an acknowledgement or more detailed reply within two working days.

To help us help you, please answer these questions in your email request, as best you can:

1. Who is the work for?
2. Why is it important?
3. What happens if the work is not done (or not done on time)?
4. What is your need (old-style accreditation on an existing contract, guidance or advice, review of proposed approach,...)?

5. What skills or experience does the work need (known or predicted)?
6. When is the next project milestone that needs cyber consultancy input or involvement?

How the team handle requests for help

Each working day, we review all new requests.

We aim to get a reply to you within two working days of us receiving the request. Some large or complex requests might need more information and discussion. These requests take extra time for us to work out the best way to support you.

Some requests might not be appropriate for the team. In such cases, we send a prompt reply, explaining why it would be better to talk with a different team. We'll usually recommend a more appropriate team, and provide contact details for them.

What happens next

If your request is not appropriate for the team, we'll tell you immediately after the initial assessment.

If your request is appropriate for the team, the assigned consultant contacts you directly. They will engage with you to start providing the help you need.

If things go wrong...

If you disagree with our decision about your request, or there is some other problem, contact us again: .

If you'd prefer a different escalation route, contact ciso@digital.justice.gov.uk.

Security culture

Security culture

This section includes material created or provided by the to help improve awareness and best practices for security within the organisation.

Note: The advice in this material cannot guarantee to protect you from problems. The range of security threats is huge, and increasing all the time.

Who is this for?

This material is for anyone who implements, administers, supports, uses or delivers services.

Christmas SMS delivery scams

Seasonal celebrations are fun, but can also suffer from scams. A common scam involves sending fake parcel delivery text messages. The messages contain fake links. The links capture personal information and bank account details. Bad actors then use these details to steal money from individuals.

Some SMS messages get people to install malware. An example is Flubot, which steals personal and banking details. Flubot also uses your contact lists to send more fake texts.

The best way to avoid SMS scams is to contact parcel delivery companies directly. Go to their website and tracking your parcel there. Never click on a link in a text message.

Information security policies

Management direction for information security

Avoiding too much security

This guidance applies to developers and system administrators who work for the .

Is it possible to have too much security? Yes. Providing too much security for things or information that do not need protection is a waste of resources. It undermines the value of the security for things that do need it.

Security by obscurity is one of the weakest approaches for protecting something. It's far better to have a technical control in place to protect the system.

Not all domain names or IP addresses in Government systems are sensitive items

An example is a domain name or IP address. These values do not need to be secret for all systems. Only those that need it. It might be tempting to say that 'all IP addresses are . This is then used as a reason for an (in)action, such as "I can't email you that network diagram because it contains IP addresses." But the statement has wider consequences. It imposes a set of security requirements for everyone. It imposes them irrespective of the actual secrecy required.

is not a different classification to . It doesn't need special technical controls or procedures. Rather, it's a reminder to look after a piece of information. It's not a controls checklist. Using labels too casually conflicts with the idea of thinking about information and what we're doing with it, and using that to decide how best to secure the information.

Of course, you might need to keep the access details for some systems secure. An example might be where you cannot maintain or patch a legacy system. But these should be exceptional or 'edge' cases.

There are only a small number of situations where you need to protect IP addresses or domain names. It's usually where the context makes the information sensitive in some way. IP addresses can be personally-identifiable information. For example, a system log file might hold the IP address of a client accessing the system. This might reveal a link between an individual and their use of services. But the IP address of a public sector server or a router should not be personal data.

Remember also that within the , system almost always have RFC1918 addresses. These are normally not routable from the Internet. If you can access the system from the Internet, then you have other problems to resolve. Address them by appropriate security measures rather than hoping that secrecy is enough.

In other words, avoid saying that 'all IP addresses and domain names must be secure'. Instead, think about and justify the handling protections around each piece of information. Ask what data or capability is actually in need of protection, and from what risks.

It's not only about domain names or IP addresses

The need to keep some aspect of a system secret might be evidence that the technical security measures around the system are not complete, adequate, or appropriate to the risks. A well-designed system won't depend on secrecy alone for security.

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

The is required to adhere (but prefers to exceed) to the Minimum Cyber Security Standard (MCSS).

The Standard

The UK HMG Security Policy Framework mandates protective security outcomes that the must achieve (and suppliers to , where they process data/information).

More information is available from https://www.gov.uk/government/publications/the-minimum-cyber-security-standard.

IDENTIFY

IDENTIFY is a prerequisite standard that requires:

- appropriate information security governance processes;
- identification and cataloguing of information held/processed; and
- identification and cataloguing of key operational services provided.

PROTECT

PROTECT is the core standard to provide fundamentally defences to information and requires:

- access to systems and information to be limited to identified, authenticated and authorised systems/users;
- systems to be proportionally protected against exploitation of known vulnerabilities; and
- highly privileged accounts (such as administrative level) to be protected from common attacks.

DETECT

DETECT is the core standard to detect when attacks are taking, or have taken, place and requires:

- capture event information (and apply common threat intelligence sources, such as CiSP);
- based on PROTECT, define and direct monitoring tactics to detect when defence measures seem to have failed;
- detection of common attack techniques (such as commonly known applications or tooling); and
- implementation of transaction monitoring solutions where systems could be vulnerable to fraud attempts.

RESPOND

RESPOND is the core standard to define the minimum of how organisations should respond to attacks and requires:

- development and maintenance of an incident response & management plan (including reporting, roles and responsibilities);
- development and maintenance of communication plans, particularly to relevant supervisory bodies, law enforcement and responsible organisations such as the NCSC;
- regular testing of the incident response & management plan;
- assessment and implementation of mitigating measures on discovery of an incident (successful attack); and
- post-incident reviews to ensure feedback into the iteration of the incident response & management plan.

RECOVER

RECOVER is the core standard to define the minimum of how organisations should recover from an attack once it has been considered closed, and requires:

- identification and testing of contingency mechanisms to ensure the continuance of critical service delivery;
- timely restoration of the service to normal operation (a plan to do so, and testing of that plan);
- from DETECT & RESPOND, immediately implementing controls to ensure the same issue cannot arise in the same way again, ensuring systematic vulnerabilities are proportional remediated.

IT Security Policy (Overview)

This policy gives an overview of information security principles and responsibilities within the and provides a summary of the 's related security policies and guides.

Audience

This policy is aimed at three audiences:

Technical users

These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Service Providers

Defined as any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the .

General users

All other staff working for the .

Within this policy, "all users" refers to General users, Technical users, and Service Providers as defined previously.

Associated documentation

For further guidance on IT Security, refer to the following policy.

- IT Security All Users Policy: which provides further details of the responsibilities of all users at the .

Principles

All users :

- Comply with the 's Acceptable Use Policy wherever they work.
- Report all security incidents promptly and in line with 's IT Security Incident Management Policy.
- Make themselves aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other guidance.
- Be aware of the need for Information Security as an integral part of the day to day business.
- Protect information assets under the control of the organisation.

Further information can be found in the IT Security All Users Policy.

Enforcement

- This policy is enforced by lower level policies, standards, procedures and guidance.
- Non-conformance with this policy could result in disciplinary action taken in accordance with the 's Disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the always co-operates with the relevant authorities, and provides appropriate evidence.

IT Security All Users Policy

Introduction

This policy provides more information on the actions expected of all users when using equipment and infrastructure. It is a sub-page to the IT Security Policy Overview.

Note: In this document, the terms "data" and "information" are used interchangeably.

Audience

This policy is aimed at three audiences:

Technical users

These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Service Providers

Defined as any other business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of, the .

General users	All other staff working for the .

Within this policy, "all users" refers to General users, Technical users, and Service Providers as defined previously.

Approach

The ensures that IT security controls are designed and implemented to protect data, IT Assets, and reputation, based around the following requirements:

Confidentiality	Knowing and ensuring that data can only be accessed by those authorised to do so.
Integrity	Knowing and ensuring the accuracy and completeness of data, and that it has not been deliberately or inadvertently modified from a previous version.
Availability	Knowing and ensuring that IT systems and data can always be accessed when required and authorised.

Assets

This policy applies to all premises, physical equipment, software and data owned or managed by the . This includes IT systems, whether developed by the or managed by IT service providers. It covers the use of IT equipment and the data processed on those IT systems, irrespective of location. It provides direction and support to preserve the confidentiality, integrity, and availability of resources.

Security classification

All Staff are responsible for ensuring data is:

- Classified correctly as detailed in the Information Classification, Handling and Security Guide
- Distributed only in accordance with the statements of this policy and related guides.
- Protected by the appropriate security controls to ensure its confidentiality, integrity and availability.

Physical and personnel security

The Physical Security Policy defines how physical access to assets must be controlled within the to prevent unauthorised access, use, modification, loss, or damage. All users must understand that:

- All IT systems and services must be assessed against environmental risks, for example flood or fire, to maintain the asset's confidentiality, integrity, and availability.
- The 's IT Teams are not directly responsible for the physical security and environment of the sites.
- Physical security controls and the environment in which the IT systems operate form part of a system's overall risk landscape. All users ensure they adhere to the security controls and requirements set out in this policy.
- Unless otherwise formally agreed by the , all users, including agency staff and contractors who have access to data, require Baseline Personnel Security Standard (BPSS) assessment, as a minimum.
- National Security Vetting should only be applied for where it is necessary, proportionate, and adds real value.
- The does not have a standing requirement for system administrators or application developers to maintain Security Check (SC) clearance.

Further information on physical and personnel security is available from and CPNI Guidance.

Identity and access control

The Access Control Guide ensures that information and IT assets can be accessed only by authorised personnel, and that each individual is accountable for their actions.

Email security

The Email guidance tells you about safe and secure use of email within the .

Remote working and portable devices

The has in place Remote Working guidance that sets out the requirements for safely accessing and using the 's systems and applications when working remotely, for example from home, another government office, or while travelling.

Mobile computing is the use of portable equipment such as mobile phone, laptop or tablet, and which supports remote working. Mobile computing equipment provided by the must be used in line with the Acceptable Use Policy.

Any request to take IT equipment overseas must follow the guidance provided in the Acceptable Use Policy and the information on accessing IT systems from overseas.

Roles and responsibilities

All users are responsible for ensuring the confidentiality, integrity, and availability of data within the . This includes all data and assets. These responsibilities extend to all assets referenced in this policy.

All users comply with the roles and responsibilities outlined in the Information Assurance Framework Process.

Specific roles and responsibilities are described within each sub-page. All users comply with these roles and responsibilities, and understand these as being a part of their ultimate responsibility for information security within the .

For the purpose of this Information Security Policy, the following roles are described. They have specific responsibilities in the implementation and monitoring of different provisions of the policy.

Role	Responsibility	Which includes...
Senior Information Risk Owners (SIROs)	The SIRO is responsible for the overall information risk policy and guidance, and ensures that the policy and guidance material continues to provide appropriate risk appetite and a suitable risk framework.	Implementing and managing information risk management in their respective business groups.
		Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.
		Authorising any exceptions and deviations from the IT Security Policy with consideration of the impact any changes might have to other users.
Delegated Agency SIROs	The delegated agency SIRO is responsible for the information risk policy and guidance as it applies to their systems and personnel, and ensures the agency adheres to the 's risk appetite and risk framework.	In line with the SIRO, but for Agency systems and personnel.
Information Asset Owners (IAO)	IAOs, also known as IA Leads, must be satisfied that all required technical, personnel, physical and procedural security controls are in place and followed. IAOs are responsible for ensuring the management and security of their information asset over the whole asset lifecycle.	Logging and monitoring.
		Reviewing access permissions.
		Understanding and addressing risks associated to their information assets.

Role	Responsibility	Which includes...
		Ensuring secure disposal of information when it is no longer required.
System Owners	System Owners are responsible for managing access control rules for their particular system.	Verifying access rights in order to assist a scheduled review audit of User accounts and permissions.
Contract Owners	Contract Owners are responsible for ensuring contractors adhere to the IT Security Policy set out here and in associated documentation.	Verify that contracts are written to reflect the 's IT Security Policy.
		Ensure contractors comply with the requirements set out by this policy and associated documentation.
		Being responsible for escalating the risk of non-compliance by a supplier, and seeking guidance on suspected non-compliance with security requirements in a contract.
		Ensure that the contractor is responsible for any sub-contractors that they employ directly or indirectly, and that the contractor, not the , is responsible for ensuring that those sub-contractors comply with this policy and associated documentation.

Line Manager approval

This guidance applies to all staff and contractors who work for the .

Some IT Policy documents need you to get a review or approval from a Line Manager or other senior person. Do this before taking an action or working in a particular way.

An example is:

- Personal Devices.

This guidance describes what you should do. The guidance contains steps to follow for Line Managers, and their Direct Reports.

Steps to follow (Line Managers)

Note: If at any time you need help about this process, or the applicable IT Policies, just ask: .

1. Check that your direct report (DR) has said what they want in their request. The request should identify which IT Policies apply.
2. Check that the request is valid from a business perspective. If not, deny the request (step 7).
3. Check that Acceptable Use is in the list of applicable policies.
4. Review the requirements or obligations within the IT Policies that apply to the request.
5. Check that the DR understands and will follow the requirements or obligations. For example, have a discussion with them, or ask them for more information or evidence.
6. If they are able to follow the applicable IT Policies, send a formal approval to the DR. An email is enough for this.
7. If you don't think they can follow the Policies, or there's a weak business case for the request, refuse it.

8. Keep a copy of your formal reply, in accord with Data Retention requirements.
9. Some IT Policies need a copy of formal approval for other parties. For example, before your DR travels to some countries on business, send a copy of your approval to .

Steps to follow (Direct Reports)

Note: If at any time you need help about this process, or the applicable IT Policies, just ask: .

1. Check that your business need is valid.
2. Check which IT Policies apply to your request. Include Acceptable Use in the list of applicable policies.
3. Check that you understand the requirements or obligations within those IT Policies.
4. Prepare evidence to show that you will follow all the requirements or obligations. Check that you have all the required information.
5. Send a formal approval request to the authorities required by the IT Policies. Ensure that you include:
   - Your request.
   - The business case.
   - The list of applicable IT Policies.
   - Evidence that you understand and can follow the requirements or obligations.
6. Be ready to have a more detailed discussion about your request, or to supply more information.
7. If you get formal approval, keep a copy, in accord with Data Retention requirements.
8. If your request is denied, check that you understand the reasons. Use this understanding to tackle your business task again, if appropriate.

Mobile devices and teleworking

Mobile device policy

Mobile Device and Remote Working Policy

Introduction

This policy gives an overview of mobile devices and remote working security principles and responsibilities within the . It provides a summary of the 's related policies and guides in relation to mobile devices and remote working.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.MOB.xxx**, where **xxx** is a unique ID number.

Audience

This policy is aimed at:

Technical users	These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
Service Providers	Any other business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services, including processing, transmitting,and storing data for, or on behalf of, the .
General users	All other staff working for the

“All users” refers to General users, Technical users, and Service Providers, as defined previously.

Mobile devices

POL.MOB.001: When using mobile devices, special care be taken to ensure that business information is not compromised. When issuing or using mobile devices, the following points be adhered to:

- **POL.MOB.002:** Mobile devices be registered as an asset.
- **POL.MOB.003:** Software installation be available for general users, except when using an approved process or tool, such as an self-service app store.
- **POL.MOB.004:** There be an ability for remote disabling, erasure or lockout.
- **POL.MOB.005:** approved web services and web apps be used.

Use in public places

POL.MOB.006: Care be taken when using mobile devices in public places, meeting rooms, and other unprotected areas. Protection be in place to avoid the unauthorised access to, or disclosure of, the information stored and processed by these devices.

The Access Control Guide explains how the manages access to its IT systems so that users have access to the material they need, in a secure manner.

Theft or loss

POL.MOB.007: Mobile devices be physically protected against theft, especially when left unattended. Examples include leaving devices unattended in cars and other forms of transport, hotel rooms, conference centres, and meeting places.

Note: Sometimes, it might feel difficult to determine a sensible level of protection. For example, leaving a laptop unattended but in plain sight on the seat of car in a public car park is not very secure. But if the car is parked in an car park, then the vehicle - and therefore its contents - are probably more secure. The answer is that you should always apply the best possible protection for the assets you are responsible for, at all times. Don't rely on other security mechanisms to provide protection that you neglected to apply.

POL.MOB.008: The have, and follow, a clear procedure covering legal, insurance, and security requirements for cases of loss or theft of mobile devices.

Use of private equipment

POL.MOB.009: You use personal devices for work purposes.

Exceptions are possible on a case-by-case basis, for example to accommodate Accessibility requirements. To discuss whether you have a case for exemption, contact the Security team in the first instance, *before* using a personal device for work purposes. If an exception is permitted, use of the personal device be in compliance with personal device guidance.

Remote working

Remote working refers to all forms of business activity that takes place outside of the office. Remote working is sometimes described as “Working From Anywhere”. Remote working locations include non-traditional work environments or contexts, such as:

- Coffee shops.
- Commuter hubs.
- Co-working spaces.
- Flexible workplace.
- Home offices or workspaces.
- Telecommuting.
- Virtual Work Environments.

POL.MOB.010: The allows remote working, but the following points be considered, confirmed, and documented as acceptable during the approval process:

- The existing physical security of the remote working site, taking into account the physical security of the building and the local environment.
- The communications security requirements, taking into account the need for remote access to the 's internal systems, the sensitivity of the information that will be accessed and passed over the communication link, and the sensitivity of the internal systems being accessed.
- Any threat of unauthorised access to information or resources from other persons using the remote working location, for example family or friends.
- The implementation of home networks, and requirements or restrictions on the configuration of wireless network services (wifi).
- Malware protection and firewall requirements.

POL.MOB.011: The guidelines and arrangements for remote working be considered, including:

- The provision of suitable equipment and storage furniture for the remote working activities.
- A definition of the work permitted, the hours of work, the classification of information that may be held, and the internal systems and services that the remote worker is authorised to access.
- The provision of hardware and software support and maintenance.
- The provision of insurance.
- The procedures for information and asset backup, and for ensuring business continuity.
- Audit and security monitoring.
- Limitation or revocation of authority and access rights, and the return of equipment when the remote working activities are terminated.

Current supporting documentation:

- Remote Working
- Security Guidance for Using a Personal Device

Enforcement

This policy is enforced by lower level policies, standards, procedures, and guidance.

Non-conformance with this policy could result in disciplinary action taken in accordance with the 's Disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the department always cooperates with the relevant authorities, and provides appropriate evidence.

Remote Working

Key points

- Be professional, and help keep information and resources safe and secure at all times.
- Think about where you are working, for example - can other people or family access what you are working on? Be thoughtful about information privacy.
- Keep accounts and password information secure.
- Take care of your equipment. Devices are more likely to be stolen or lost when working away from the office or home.
- Get in touch quickly to report problems or security questions.
- Use the VPN if you are handling sensitive information, or connecting to systems from a remote location.
- Send work material to personal email accounts.
- Use personal devices or accounts for work purposes - the exception is that a home wifi connection may be used to connect equipment.
- Leave equipment unattended.

Overview

The Remote Working Guide gives you advice and guidance on the main security issues that are likely to affect you as a remote worker or a user of mobile computing facilities, (e.g. desktop/laptop computer, smart phones, etc), within the , including its Agencies and Associated Offices.

It also sets out your individual responsibilities for IT security when working remotely.

Audience

This guide applies to all staff in the , its Agencies, Associated Offices and Arm's Length Bodies (ALBs), including contractors, agency and casual staff and service providers, who use computing equipment provided by the Department for remote working or mobile computing, or process any departmental information while working remotely or while using mobile computing equipment.

What is remote working?

Remote working means you are working away from the office. This could be from home, at another or government office, whilst travelling, at a conference, or in a hotel.

Protecting your workspace and equipment

Remote working is when you work from any non- location, for example, working at home. It's important to think about confidentiality, integrity and availability aspects as you work. This means protecting equipment, and the area where you work.

- Keep equipment and information safe and secure.
- Protect information from accidental access by unauthorised people.
- Lock or log off your device when leaving it unattended. For long periods of non-use, shut down your device.
- Ensure that your devices are powered off when you first enter a country when travelling outside the UK.
- Keep your workspace clear and tidy. Follow a 'clear desk policy' for information, including paperwork, to ensure information isn't seen by unauthorised people.
- Use IT equipment for business purposes in preference to your own equipment such as laptops or printers.
- Be wary of anyone overlooking or eavesdropping what you are doing. Consider whether you, or the information, might be Overseen, Overheard, or Overshared.
- Protect chargers and other computer accessories, especially equipment, when travelling. This is to prevent them from being tampered with. Keep them secure and out of sight as much as possible, for example in your hand luggage or on your person.
- Ensure that a laptop BitLocker PIN or similar access control is enabled.
- Use an -issued VPN when connecting to Hotel or other public wifi spots.
- Let family or other unauthorised people use equipment.
- Leave equipment unattended.
- Work on sensitive information in public spaces, or where your equipment can be seen by others.
- Advertise the fact that you work with materials. However, pre-installed materials such as backgrounds provided as standard with equipment are acceptable.
- Take part in conference or video calls when you are in public or shared spaces such as cafes or waiting rooms.
- Send your work material to your personal devices or your personal email address.
- Redirect print jobs from printers to a personal printer.
- Use public 'charging stations' provided at airports, conference venues, hotels, or similar public locations. They might be used to upload malicious software onto your device.
- Connect equipment to vehicles, using either USB or Bluetooth. These connections can download information from the device or upload malicious software.

Working securely

It's important to consider the security of how you work remotely.

- **Work locations** - as with home working discussed previously, you need to be equally, if not more, vigilant when working in public spaces.
- **Confidentiality** - be aware of others eavesdropping or shoulder surfing, both what you are working on and what you are saying, for example during conference and video calls.
- Keep **equipment and information**, including printouts and documents, safe and secure.

Even when working remotely, you must still follow the security policies and operating procedures for systems you access and work with.

Using public wifi or internet, and home broadband

Some locations, such as hotels, coffee shops, or public transport, offer 'public' wifi or internet access.

The public services are usually offered for free. They only need you to agree to some terms of service.

While apparently convenient, these services can have some serious problems:

- They have no security appropriate for protecting information.
- There is no guarantee about keeping information transmitted through them private or confidential.
- Public services are usually shared. This means that performance can often be very slow and unreliable.

If you need network access, but cannot connect to an network or home broadband service:

- Use an hotspot. This is usually provided on your -issued mobile device.

If you need to use a public wifi or internet service, or home broadband, with your equipment, because you do not have an hotspot, then:

- Connect using an -issued VPN. Before doing any work, check that the -issued VPN is working correctly.

Using your own equipment

The main guidance is available here.

- Use official equipment for business purposes.
- Send your work material to your personal devices or your email accounts.

If you are working remotely, or do not have access to equipment, it might be tempting to use your own equipment, especially printers. Avoid doing this.

Printing

The advice is to avoid printing anything when working remotely, and in particular not to use personal printers.

However, if you really must print information:

- Connect directly to the printer using USB, not wifi.
- Consult the information asset owner or line manager before printing the information.
- Store any and all printed materials safely and securely until you return to premises, when they must be disposed of or filed appropriately.
- Print out personal information relating to others.
- Redirect print jobs from an printer to a personal printer.
- Dispose of unshredded information in your home rubbish or recycling. Use a cross-cut shredder to destroy printed materials securely, before disposal at non- locations.

Basically, think before you print.

Privacy

It is important to protect privacy: yours and that of the . Events like the Covid-19 (Coronavirus) pandemic are often exploited by people wanting to get access to sensitive or valuable information. This often results in an increase in attempts to get access to personal information or accounts, using phishing and email scams. Be extra vigilant whenever you get an unexpected communication.

Be aware of your working environment when you work with information. If anyone might access the data, or hear you talk about it as you use it, that could cause privacy problems. Be aware of SMART devices around your remote location, and ensure they are switched off if conducting video or voice communications.

Guidance and suggestions for improving Privacy appear throughout this guide, but it's worthwhile highlighting these points:

- Lock your computer, even when unattended for short periods.
- Think about whether an unauthorised person, such as a family member, might access the information you are working with.
- Write down passwords. Use a password manager.

Contacts for getting help

In practice, all sorts of things can go wrong from time-to-time. Don't be afraid to report incidents and issues; you will be creating a better and safer work environment.

Related information

NCSC Home working: preparing your organisation and staff CPNI Home Working Advice

To access the following link, you'll need to be connected to the HMPPS Intranet.

HMPPS Advice

Teleworking

Personal devices

This guidance applies to all staff and contractors who work for the . It provides advice about using personal devices for work purposes.

Related information

Bluetooth on page 80

Overview

A personal device is any desktop, laptop, tablet, phone, external drive, or similar device that the does not own.

Note: 'Personal devices' include all personally-owned devices with processing ability or Internet connectivity. This includes all types of assistance, organisational or Internet of Things (IoT) devices. Connected vehicles are a special case discussed in this guidance. In case of any doubt, ask for help about specific examples.

Not everyone has access to an device for remote use. If you need equipment, you can request it. It can be provided quickly. Contact your Line Manager for details. A request can then be raised through the .

In unusual circumstances, it might not be possible to organise provision of equipment. In such cases, you request access to an virtual environment.

Except when connecting to an virtual environment, or with documented approval in exceptional circumstances as described in this guidance, you use a personal device for work purposes.

Avoid connecting peripherals to devices, unless those peripherals are supplied or approved by the . Examples of peripheral devices include USB, wireless, or Bluetooth keyboards or mice.

Note: Exemptions are possible for connecting peripherals where accessibility support is required. Contact your Line Manager for documented approval before connecting a peripheral device.

Personal devices be charged from the USB ports of an device.

Note: Specifically: a personal mobile phone be charged from the USB ports of an device.

Guidance

- If you have an -issued device or virtual environment, you use that.
- You use a personal device to access tools such as Gmail, Docs, Slides, Sheets, Drive, Meet, or Hangouts for work purposes.
- You use a personal device to access Office 365 tools such as Outlook email or calendar, Word, Excel, or PowerPoint for work purposes.
  - Wherever possible, an work device be used to join business Teams calls, either via video or dial in.
  - In cases where staff have not been provided with a work phone or laptop or any other work device which allows them to join or dial into Teams, staff join from their personal devices as a Guest. The chair of the meeting confirm the identity of each and every person joining their call as a Guest.
- This guidance applies to all tools accessed through a web browser or installed client applications.

- You send information to your personal email account.
- You use personal accounts for work purposes.
- You store work files or information on a personal device such as a desktop, laptop, tablet or phone.
- You store work files or information on a personal storage device or memory stick, such as an external drive, thumb drive, or USB stick.
- Some teams within the have permission to use personal devices for some tasks. This permission continues, but is being reviewed on an on-going basis. Ensure that you have documented approval recording your permission. Ensure that the permission is no more than 12 months old. To request or refresh permission, ask your Line Manager to seek approval by checking with the .

Note: You are not asked or required to use your own devices for work purposes. Statement **POL.MOB.009** of the mobile device and remote working policy makes clear that you use personal devices for work purposes. If you have access to devices for work purposes, you use them by default. A special case is that if you do not have an -issued mobile phone, you use a personal device to receive Multi-factor authentication (MFA) codes or messages which authorise access by devices to systems.

Using tools on personal devices

In accordance with other policy on the use of personal devices, and the use of mobile devices specifically, you use personal devices to access tools, such as Slack workspaces.

Note: The rest of this section refers to Slack workspaces, but applies equally to other tools, such as Teams, Trello, Jira, and so on.

You could of course use personal devices to access other (non-) Slack communities.

The point is that you use personal devices for work purposes. Slack workspaces are official workspaces and only be accessed using devices.

Personal devices are not allowed to access services or content containing data. Work devices be used to access services such as Slack communities. If you do not have a work mobile device, and need to access services such as Slack on a mobile device, you request one using Service Now.

Virtual environment

The provides access to a Virtual Environment to help with exceptional circumstances. This is where suitable provision of a physical device is not possible.

Request a virtual environment through the `Creation of WVD instances` product offering within the Service Catalogue in Service Now.

Note: A virtual environment does not offer the same capabilities or performance as a physical -issued device. Using an -issued device is always preferable.

Connected vehicles

Connected vehicles are effectively Bluetooth-connected storage devices. They are considered personal devices for the purposes of this guidance, regardless of whether they are owned, leased or rented.

Automatic transfer of contact information and calendar events might happen during the pairing process. The resulting transferred data is accessible to any third party who subsequently pairs their mobile device to the vehicle.

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. Transferred information might not be immediately visible or accessible, but this is not the same as deleting the information from the vehicle.

For these reasons, devices be paired with Bluetooth-enabled vehicles.

Human resource security

Prior to employment

Minimum User Clearance Requirements Guide

This Minimum User Clearance Requirements Guide outlines the level of security clearance required for staff in order to access specific account types.

Security clearance levels

The uses the national security vetting clearance levels:

- Baseline Personnel Security Standard (BPSS)
- Counter Terrorist Check (CTC)
- Security Check (SC)
- Developed Vetting (DV)

Where appropriate, Enhanced checks apply, for example Enhanced Security Check (eSC).

Minimum user clearance requirements

Most of the IT systems are able to process information. Therefore all roles in the require staff to attain BPSS clearance as a minimum to be granted access rights to view information. Some roles require staff to have higher clearance.

For an individual to perform any of the following tasks, clearance higher than BPSS is required:

- Has long term, regular, unsupervised access to data centres or communications rooms.
- Has regular privileged unsupervised and unconstrained access to systems which contain data for multiple systems, for example backups, or console access to multiple cloud services.
- Has cryptography responsibilities and handling, under advice from the Crypto Custodian.
- Has access to multiple system security testing outcomes which reveal vulnerabilities in live services.
- Has a role such as system support or IT investigation role, such that without further authority or authorisation, an individual might:
  - Act as another user.
  - Obtain credentials for another user.
  - Directly access other users' data.

If an individual does not need to perform any of the previous tasks, then BPSS, DBS or Enhanced Check is sufficient.

The HQ and Executive Agencies might have additional, specific requirements for DV/DV STRAP clearance for individual systems. These requirements should be followed where applicable.

Please contact the for further information.

During employment

Training and Education

Overview

This information applies to anyone and everyone working for, or with, the .

The 's Information Security awareness programme plays an essential part in maintaining security. It informs all staff of:

- Their duties with regard to security.
- Their responsibilities to protect the assets (information, equipment, people and buildings) they have access to and use.
- The importance of reporting any actual or suspected security incidents.

Requirements

All staff starting or returning to work within the receive mandatory security training.

The objective is to ensure that all new and current staff members are aware of their security responsibilities whilst working at the .

Full details of the mandatory training are provided in the Joiner, Mover, and Leaver pages on the Intranet.

In summary, as a minimum everyone :

- Have taken and completed an Security induction.
- Have completed the Civil Service Learning course on "Responsible for Information (RfI)", or an approved equivalent.

Normally, this training be completed successfully before accessing information, resources, or assets.

Termination and change of employment

End or change of employment

Managers must ensure that all employees, contractors and third-party users return all assets within their possession and that all access rights (including building passes, access to buildings, IT systems, applications and directories) are removed at the point of termination or change of employment.

If the leaver has security clearance, managers should contact the to advise that the person has resigned and tell them their leaving date or the date on which they will be moving to a different department.

Leavers should read the HR guidance at End or change employment.

Managers must also complete a leaver's checklist as a record of actions.

Downloads

Leavers checklist

A downloadable version of the "End or change of employment" document is available here.

Asset management

Responsibility for assets

Acceptable use of Information Technology at work

This guidance applies to all staff and contractors who work for the .

Everyone working at the has access to Information Technology (IT) resources. You must use them in an acceptable way. This guidance explains what that means. The definitive list of Acceptable Use Policy statements is here.

Summary

Be sensible when using IT resources:

- The resources are for you to do work.
- Protect the resources at all times, to help prevent unacceptable use.
- If the use would cause problems, upset, offence, or embarrassment, it's probably not acceptable.
- Context is important. Security risks can increase when working outside your normal workplace.
- Be aware that your use of resources is monitored. During an investigation into a security incident, IT forensic techniques capture evidence.
- If you're not sure if something is acceptable, ask for help first.
- Above all, if you think there is a problem, report it or ask for help.

The way you use IT is important, because it indicates your approach to work, and can be taken into account when assessing your behaviour and performance.

What is meant by IT?

IT means the devices or services you use for creating, storing, or sharing information. This includes everything from devices (such as laptops, 'phones, mobile Wi-Fi hotspots (MiFi), iPads, tablets, printers, USB "memory sticks") through to online services (citizen-facing online services, staff tools, corporate email).

Acceptable use of IT

Acceptable use of IT is when you use it to do your work.

IT helps you complete your tasks as efficiently and effectively as possible. Sometimes, you might need account details such as passwords to use the IT. Acceptable use means protecting this kind of information, too.

Acceptable use can also vary according to context. For example, checking sensitive personal details might be perfectly normal within a secured office, but is not acceptable in a public space where anyone else might access those details.

Unacceptable use of IT

Unacceptable use of IT prevents you or your colleagues from doing work, or is unlawful or illegal, or does not take the context into account.

There are many unacceptable uses of IT, making it impossible to provide a complete list. Examples of things to avoid include:

- Deliberately or accidentally sharing resources or information, such as passwords, with people who are not supposed to have them.
- Using resources without permission.
- Storing sensitive information where it could easily be lost or stolen.
- Using unapproved tools or processes to store sensitive information, such as passwords or credit card details.
- Using your work email address for personal tasks.
- Using your personal devices or your personal email address for work tasks.
- Excessive private use during working time.
- Installing unlicensed or unauthorised software.
- Redirecting print jobs from printers to a personal printer.
- Sending your work material to your personal devices or your personal email accounts. (It is of course acceptable and necessary from time-to-time to send work material to someone else's email address when they are directly involved with that work, for example someone in the Office of the Public Guardian (OPG) emailing someone regarding Lasting Power of Attorney (LPA).)

Why unacceptable use is a problem

Unacceptable use of IT might affect the in several ways, such as:

- Bad publicity or embarrassment.

- Increased or unexpected costs or delays.
- Civil or legal action.
- Reduced efficiency and effectiveness.

Unacceptable use might also affect you, too:

- Suspension of access, so that you cannot do your work.
- Disciplinary proceedings, up to and including dismissal.
- Termination of contract for contractors and agency staff.

Keeping control

You are responsible for protecting your IT resources. This includes keeping your usernames and passwords safe and secure.

It also means looking after equipment, especially when working away from locations. You are responsible for protecting equipment issued to you. Any theft of equipment, or deliberate or wilful damage to equipment, should normally be reported to the Police and to the .

Note: You should normally report instances of theft or damage to authorities as indicated. However, there might be additional circumstances which mean a sensitive handling of the situation is appropriate. It is acceptable to consider the context of the situation when making a report. Ensure you can justify your actions. In cases of uncertainty, don't hesitate to ask your line manager, or other responsible authority for advice.

While you might be careful about acceptable use of IT, there are still risks from malware, ransomware, or phishing attacks.

If you get an email from anyone or anywhere that you are not sure about, remember:

- Don't open any attachments.
- Don't click on any links in the email.

If there is any doubt, or you are worried that the email might be malicious or inappropriate, report it immediately as an IT security incident.

Personal use of IT

Limited personal use of IT is acceptable as long as it does not cause a problem with your work or that of your colleagues. Context is important. For example, doing personal internet banking during your lunch break might be acceptable, but doing the same thing during a work meeting would not.

Personal use of mobile phones

You might be allocated a mobile phone for use as part of your work. The mobile phone enables you to:

- Make or receive calls.
- Send or receive SMS texts.
- Use Internet services.

This usage must always be for work purposes.

Examples of unacceptable mobile phone use include:

- Making charitable donations from the mobile phone account.
- Signing up for premium rate text services.
- Calling premium rate telephone services.
- Voting in "reality TV" popularity contests - these usually involve premium rate services.
- Downloading, uploading, or streaming media files that are not work-related, such as music or movies.
- "Tethering" another device to the mobile phone, and then using the other device for any of the previously mentioned activities.

... as well as any other activities that are not obviously work-related.

All use of IT resources is monitored and logged. This includes mobile phone usage listed in account bills. It is possible to find out if you used a work-issued mobile phone for unacceptable activities. Unacceptable use is reported to your Line Manager for further appropriate action. Assessing your behaviour and performance takes this kind of activity into account.

Using IT outside your usual workplace

Some IT resources might be usable away from your usual workplace, such as a laptop. Even outside the office, you must continue to ensure acceptable use of the IT resources.

You should also ask before taking IT equipment outside the UK.

Avoid using removable media

Removable media like memory sticks are portable and easy-to-use. Unfortunately, this makes them a security risk, so avoid using them. If however they are essential to your work, follow the Use of Removable Media guidance.

Personalisation of equipment

A popular trend is to adorn laptops with stickers. This is acceptable as long as the material does not cause problems such as upset, offence, or embarrassment. The same applies if you customise the desktop environment of your equipment, for example by changing the desktop image.

Acceptable Use Policy

This document is the Acceptable Use Policy. It provides the core set of security principles and expectations on the acceptable use of IT systems.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.ITAUP.xxx**, where **xxx** is a unique ID number.

Introduction

IT systems and services are first and foremost provided to support the delivery of the 's business services. To achieve this, most users are provided with an appropriate general purpose computer environment, and access to services and communication tools such as email and the Internet.

This policy outlines the acceptable use of IT systems and services, and the expectations that the has on its staff when accessing or using those systems or services.

Scope

This policy covers all Users (including contractors and agency staff) who use IT systems or services.

Failure to adhere to this policy result in:

- Suspension of access to IT systems and services.
- For employees, disciplinary proceedings up to and including dismissal.
- For others with access to IT systems and services, including specifically contractors and agency staff, termination of contract.

POL.ITAUP.001: All Users be made aware of the Acceptable Use Policy (this document), and provided with security awareness training which covers this policy.

POL.ITAUP.002: All Users undergo refresher security awareness training covering this policy, every 12 months.

Protection of assets

It is paramount that all Users protect the confidentiality of information held on, processed, and transmitted by IT systems. All Users have a role in protecting the information assets which are under their control, or that they have access to.

IT systems have been designed to protect the confidentiality of the data held on them. However, maintaining this requires the application of, and adherence to, a clear set of operating procedures by all Users. These are collectively known as Security Operating Procedures (SyOPs).

It is important that all Users of an IT system, including support and system administrative Users, are familiar with these SyOPs, and are provided with the appropriate training.

POL.ITAUP.003: All IT systems have, and maintain, a set of Security Operating Procedures (SyOPs). For systems undergoing an assurance process, these SyOPs be included as part of the assurance.

POL.ITAUP.004: All Users of an IT system, including support and system administrative staff, read the applicable SyOPs, and acknowledge that they have both read and understood the SyOPs before being granted access. A record be kept of a User being granted access, and made available for review during assurance, or upon authorised request.

POL.ITAUP.005: All Users be made aware that non-conformance to the system SyOPs constitutes a breach of the IT Security Policy, and result in disciplinary action.

POL.ITAUP.006: Any change to an IT system's SyOPs be approved through an assured change control process, before the change is made.

POL.ITAUP.007: Any request to perform an action on an IT system which contravenes its SyOPs be approved by the before the action is taken.

For most Users, access to IT systems and information held on them is through a desktop device, a laptop, or a mobile or remote device. These devices have the capacity to store large amounts of potentially sensitive information assets. It is important that Users follow Information Management processes and handling guidelines to ensure information is stored and accessed appropriately. Further information on information handling is provided in the Information Classification and Handling Policy.

General Security Operating Procedures (SyOPs)

The policy refers to a key set of general SyOPs, as follows:

- Remote Working.

To minimise the number of SyOPs in circulation and standardise procedures, the SyOPs listed previously act as the primary set, which individual IT systems are expected to conform to, in terms of their own SyOPs. Any deviations or additions are dependent upon approval through the assurance process.

POL.ITAUP.008: All IT systems have documented SyOPs which comply with the general SyOPs listed in this policy. Any deviations or additions be recorded in separate SyOPs which form an addendum to one of the SyOPs listed.

Note: An IT system make use of, in their entirety, one or more of the SyOPs listed in this policy if the procedures of that IT system do not deviate from those described in the general SyOPs.

Removable Media

Removable storage media include devices such as USB memory sticks, writeable CDs or DVDs, and external drives. These devices contain large amounts of protectively marked data, and so pose a significant risk to the confidentiality of the data they hold. As such, the controls the use of removable media through SyOPs, technical security controls, and by requiring movements of bulk data to be authorised .

POL.ITAUP.009: Any removable media device be approved by security, where that device is used to store protectively marked data. The type of device and associated SyOPs be approved by security before operational use.

POL.ITAUP.010: All Users ensure that all data stored on or transported by removable media is in accordance with the applicable system SyOPs.

POL.ITAUP.011: All Users seek approval from the prior to any bulk transfer of protectively marked data using removable media. security advises on any technical and procedural requirements, such as data encryption and handling arrangements.

Passwords

A username and password combination is the primary access credential used for authenticating a User to systems, and authorising User access to information assets and services provided by that system. It is therefore important that Users keep their access credentials safe and secure.

POL.ITAUP.012: All Users share or disclose any passwords with any other person.

POL.ITAUP.013: All Users :

- Attempt to gain unauthorised access to another User's IT account.
- Attempt to use another Users access credentials to gain access to an system.
- Attempt to access information for which they do not have a 'need-to-know'.
- Use the same password on more than one system.

Legal and regulatory requirements

There are a number of legal and regulatory requirements that the must comply with. These obligations are in addition to HMG security policy, as expressed in the HMG Security Policy Framework.

POL.ITAUP.014: All Users be made aware of legal and regulatory requirements that they adhere to when accessing systems. These requirements be included as part of the SyOPs.

Corporate Image

Communications sent from systems, or products developed using them, such as branded documents or presentations, damage the public image of the if they are for purposes not in the interest of the , or they are abusive, offensive, defamatory, obscene, or indecent, or of such a nature as to bring the or any its employees into disrepute.

POL.ITAUP.015: All Users ensure that systems are not used in an abusive, offensive, defamatory, obscene, or indecent way, or are of such a nature as to bring the or any its employees into disrepute.

Potential to cause offence and harm

The has a duty of care to all staff, and to provide a positive working environment. Part of this duty involves ensuring all staff maintain a high standard of behaviour and conduct.

POL.ITAUP.016: systems be used for any activity that causes offence to employees, customers, suppliers, partners, or visitors, or used in a way that violates the Code of Conduct.

Personal use

The permits limited personal use of its IT systems, provided this use does not conflict or interfere with normal business activities. The monitors the use of its IT systems. Any personal use is subject to monitoring and auditing, and also be retained in backup format, even after deletion from live systems.

The reserves the right to restrict personal use of its IT systems. The main methods employed are:

- Filtering of Internet and email traffic. All Internet and email traffic is filtered and analysed. Further details are available.
- Policy and procedures. This policy and associated SyOPs set out the restrictions placed on the use of systems.

POL.ITAUP.017: Users ensure that any personal use of systems does not conflict or interfere with normal business activities. Any conflict be reported to the User's line manager.

POL.ITAUP.018: Users ensure that any personal use of systems is consistent with any applicable SyOPs, and with this acceptable use policy.

POL.ITAUP.019: Users be aware that any personal use of systems which contravenes any applicable SyOPs, or this acceptable use policy, constitutes a breach of the IT Security Policy and result in disciplinary action.

Maintaining system and data integrity

Users comply with all applicable operating procedures, and ensure that they do not circumvent any security controls in place. Changes to the configuration of an IT system which affect either the integrity of that system or the integrity of shared data be undertaken or supervised by an authorised User or system Administrator.

POL.ITAUP.020: All Users request any changes to systems or equipment through the .

Electronic messaging and use of the Internet

Due to the risks associated with electronic communications such as email and the Internet, the controls and monitors usage of systems in accordance with applicable legal and regulatory requirements.

IT systems are designed to protect the from Internet-borne attacks, to reduce the risk of information being leaked or compromised, and to support the in providing a safe working environment. This is mainly achieved through the filtering and monitoring of all Internet and email traffic.

Also, the use of any high bandwidth services, such as video streaming websites, create network capacity issues, causing poor performance affecting important services. Therefore, the restricts access to the Internet, based on job role. Amendments can be made on the submissions of a business case for approval by the .

The regards as a disciplinary offence any usage of electric communications, such as email and other methods including instant messaging and the Internet, which breaks the law, contravenes HR policies, or involves unauthorised access to or handling of material that is deemed to be inappropriate, abusive, offensive, defamatory, obscene, or indecent.

External email and the Internet are, in general, insecure services where it is possible for external entities to intercept, monitor, change, 'spoof', or otherwise interfere with legitimate content. The deploys a number of security controls to protect its Users from Internet- and email-borne attacks. However, these controls are reliant on Users remaining vigilant, following any applicable SyOPs, and reporting any suspicious behaviour.

POL.ITAUP.021: All Users use the Internet, email, and other electronic communication systems only in accordance with this acceptable use policy document.

Managing email use

Users are responsible for ensuring that all information is handled in line with the protective marking of that information, in accordance with the Information Classification and Handling Policy.

The is connected to the Government network, which provides a secure environment for sending or receiving emails between Government departments. This allows Users with an email account (normally with the suffix '`@justice.gov.uk`') to send emails with handling caveats such as to another or government User, where their email suffix ends in '`gov.uk`'.

POL.ITAUP.022: All Users ensure that information contained within or attached to an email is handled in accordance with the Information Classification and Handling Policy.

Email is a major source of malware, and a route into the for criminal organisations. It be used to defraud staff, or to exfiltrate information. All Users exercise care when handling emails, and report any suspicious activity as an IT security incident.

POL.ITAUP.023: All Users ensure that they do not:

- Open any attachments to an email where the source is untrusted, unknown, or unsolicited.
- Click on any links within an email, where the source is untrusted, unknown, or unsolicited.

POL.ITAUP.024: Where a User suspects that an email received is from an untrusted, unknown, or unsolicited source, they report it as an IT security incident.

Connectivity and remote access

Remote access is provided to systems and services, allowing Users access from offsite and home locations to connect in. The main methods of access are either via a laptop or other mobile device. Normally, remote access is to a protected IT system. Users be aware of the security controls and procedures of the devices and systems being used, as well as any applicable general physical security considerations. This includes any restriction on the carriage of such devices, as they contain HMG protectively marked data, or HMG cryptographic material.

security maintains a list of countries where carriage and use of remote access devices is permitted.

Further details can be found in the Remote Working guidance.

POL.ITAUP.025: All Users be aware of the Remote Working guidance, and confirm that they have read and understood it before being provided with any remote access devices or equipment, such as an encryption or access control token.

POL.ITAUP.026: Any User wishing to take a remote access device out of the UK consult the Remote Working guidance before doing so, and the applicable device IT Security Operating Procedures document.

Monitoring of communications

Communications be monitored without notice, and on a continual basis, for a number of reasons. These include compliance with legal obligations, effective maintenance of IT systems, preventing or detecting unauthorised use or criminal activities such as cyber-intrusion, monitoring of service or performance standards, providing evidence of business transactions, and checking adherence to policies, procedures, and contracts.

The monitors telephone usage, network, email, and Internet traffic data, including sender, receiver, subject, attachments to an email, numbers called, duration of calls, the domain names of websites visited, the duration of visits, and files uploaded or downloaded from the Internet, at a network level.

The , so far as possible and appropriate, respects User privacy and autonomy whilst they are working, but in accordance with the personal use information, any personal use of systems is also subject to monitoring. By carrying out personal activities using systems, Users are consenting to the processing any sensitive personal data which be revealed by such monitoring, such as regular visits to a set of websites.

For the purposes of business continuity, it be necessary for the to access business communications, including within email mailboxes, while a User is absent from work, including for a holiday and because of illness. Access is only granted through submission of a formal request to the , where approval is required from the relevant line manager. The and HR are normally consulted as well, before access is granted.

POL.ITAUP.027: All Users be aware that their electronic communications are being monitored in accordance with this acceptable use policy.

POL.ITAUP.028: All Users be aware that business communication such as email mailboxes be accessed if they are absent from work. This access is normally requested through, and authorised by, the User's line manager. The and HR are normally consulted as well, before access is granted.

Data protection considerations

Acceptable use considerations apply to the storage of personal data. This storage includes data hosting in 'cloud' environments, or within services or databases hosted or administered outside:

- The UK.
- The European Economic Area (EEA).
- Countries with an Adequacy Decision (an 'Adequacy Decision Country' or ADC).

POL.ITAUP.029: The default position is that personal data be transferred to or through, or stored, in the US or elsewhere outside the UK, EEA, or an ADC, other than in exceptional circumstances.

This position also applies where a supplier uses cloud storage facilities in the UK, EEA, or an ADC, but their employees outside the UK, EEA, or the ADC are able to view the information for activities such as maintenance or trouble-shooting. The effect of this access is equivalent to the personal data being held outside the UK, EEA, or an ADC.

The reason for this position is that even with additional contractual clauses, the cannot ensure protection of its personal data stored outside the UK, EEA, or an ADC, due to some government surveillance laws.

POL.ITAUP.030: A supplier based in the UK, EEA, or an ADC, and which stores client data in the UK, EEA, or an ADC, be considered first and preferred where possible.

POL.ITAUP.031: If an alternative supplier cannot be sourced, then a Standard Contractual Clause (SCC) and a Transfer Impact Assessment (TIA) be completed.

These documents are reviewed by the , after which the transfer be approved. A template for these documents can be requested from

POL.ITAUP.032: If the outcome of the assessment does not support the transfer and storage of information outside the UK, EEA, or an ADC, the Information Security and Risk (ISR) Board review the case, and if appropriate, accept the risks in order for the supplier to be used.

POL.ITAUP.033: This acceptable use policy for personal data apply to:

- An existing supplier changing the location of its servers, storage, or services outside the UK, EEA, or an ADC.
- New suppliers.

Data protection acceptable use protocols and standard operating procedures

The has produced a number of Acceptable Use protocol documents, providing specific data protection guidance.

The documents are available on the Intranet, or by contacting the .

The documents are as follows:

- Acceptable Use Protocol Commercial and Contract Management
- Acceptable Use Protocol Subject Access Requests
- Acceptable Use Protocol Storage of Personal Data
- Acceptable Use Protocol Data Subjects' Rights
- Acceptable Use Protocol Processing of People Data
- Acceptable Use Protocol Analytical Platform
- Acceptable Use Protocol Recording

There are also a number of Standard Operating Procedures (SOP)s, including:

- Personal Data Risk Management
- Data protection impact assessment guidance
- Data sharing agreement assessment

For more information on these protocols and procedures, contact the .

Guidance on IT Accounts and Assets for Long Term Leave

Audience and Document Purpose

This document is intended for line managers who have a staff member going on any type of long-term secondment, loan, or leave. It provides guidance on how to handle the IT accounts and IT assets (such as desktops, laptops, or mobile phones) of the staff member while they are on leave.

Long term means longer than 2 months.

Types of secondment, loan, or leave where this might apply include:

- Adoption Leave.
- Career Break.
- Loan.
- Maternity Leave.
- Secondment.
- Shared Parental Leave.

For the purpose of this guidance, all of these are examples of "long-term leave".

Guidance Statement

Retaining assets, and access during leave

This guidance applies to assets, defined as being laptops, desktops, or mobile phones.

- A staff member going on any long-term leave may keep their assets while they remain contractually employed by the , **AND** where the leave is not longer than 12 months in duration.
- Remind your staff member that the Acceptable Usage Policy applies at all times during their leave. The policy can be found here.
- Preparation or return from any type of leave may be accompanied by changes in working patterns. The Remote Working guidance provides useful advice for anyone who may be working remotely for the first time. The policy can be found here.

Note: Devices that are not used for 3 months or more go in to a technical "quarantine", intentionally to render them unusable. Staff members should log in to their devices once per month during leave, to ensure that technical quarantine is not activated. Logging in also helps ensure that system updates are downloaded and applied.

Reviewing access to data and information systems

Before the staff member goes on leave, review their access to data and information systems, to ensure that this meets an ongoing need. This means that:

- If the staff member's role is planned to change on their return to the , consider removing access now to data and information systems which they will no longer need. If their role is not planned to change on their return, you might consider leaving access "as-is" currently.
- Consider removing access to data or information systems which are . This is in line with the necessity rigorously to apply the "need to know" principle for information. Refer to the guidance on classifying information for more detail https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/

When to remove access and return assets

In a number of circumstances assets should be returned and access should be removed. This is where:

- The leave is longer in duration, and there is no business need or individual need for the user to keep assets and access. This should be considered for any leave more than 12 months in duration. This is likely to be for Career Breaks or Loans.
- The staff member has no means of securely storing the asset, for example locking it securely in their home.
- Staff members going on leave for less than 12 months may return their assets and have access removed if they choose to do so.
- Line managers are empowered to determine whether the staff member should keep assets and access, as long as there is appropriate business justification, and staff members are appropriately supported. For example, a communication mechanism for keeping in touch is agreed.
- If, during their leave, the staff member decides to end their employment (resign), their line manager is responsible for following the appropriate leaver's process with them. Refer to the Resignation section of the HR guidance and forms, with particular reference to the Leavers Checklist for Managers. This can be found at: https://intranet.justice.gov.uk/guidance/hr/end-change-of-employment/resignation/

How to remove access and return assets

- Access to systems and return of assets can be organised through the appropriate items in the Technology Portal. Please refer to the Knowledge Base article on "Returning your laptop, accessories and mobile phones" for details. Removal of access to local systems should be arranged with local IT teams.

Note: When a Dom1 account is deactivated, its data is recoverable for up to 12 months. Refer to the Knowledge Base article on "How to Re-instate a Deactivated Email Account or Mailbox".

Protect yourself online

There are five simple things we can all do to protect ourselves online:

1. Use a strong password to protect your laptop, computer and mobile devices. To choose a good password, follow NCSC guidance.
2. Think before clicking on links or attachments within emails. By hovering your cursor over the link you can find the actual URL. If you are unsure if an email is genuine, contact your IT or security team.
3. Do not use your work email address to register for accounts on websites for personal use. For example, a shopping website does not need your work email address. Using the wrong address could open up your work email account to spam and fraudulent emails. This in turn could harm your department's IT system.
4. Protect your online identity. Do not share sensitive information about your work on social media or online professional networks.
5. Do not disclose your level of vetting. If you share this information, you advertise what resources you have access to. This could make you a target for malicious individuals.

For more information, refer to the Acceptable Use guidance.

Information classification

Data Handling and Information Sharing Guide

This guide is designed to help protect information held on IT systems, by providing guidance on how it should be handled and shared in a safe and secure manner.

Overview

Introduction

The identifies mandatory requirements about the value and classification of information assets. To comply with these requirements, the needs to ensure that:

> Where information is shared for business purposes, departments and agencies ensure the receiving party understands the obligations and protects the assets appropriately.

and

> All staff handling sensitive government assets are briefed about how legislation (particularly regarding Freedom of Information and Data Protection) specifically relates to their role, including the potential disciplinary or criminal penalties that may result from failure to comply with security policies. Appropriate management structures be in place to ensure the proper handling, control and (if appropriate) managed disclosure of sensitive assets.

The policy on data handling and information sharing is covered in the Information Classification and Handling Policy, whilst this document sets out the guidance sharing information within the and externally with other Government departments and 3rd parties.

Note: Other guidance might refer to information classified as being `IL3 REST*`. This is an older classification standard. In general, `IL3 REST*` is approximately equivalent to with the handling caveat, often written as. While this approximate alignment might be helpful, you should always review classification where older terms are used, to ensure that the correct current classification is used.

Scope

This document provides guidance on handling or sharing information stored on IT systems, or exchanged electronically within the , or with external parties.

The can help you with more guidance on the handling of protectively marked data.

This guide is split into three sections:

- Handling data on IT systems.
- Information sharing.
- Reporting data loss.

Note: This document provides guidance for handling and sharing of information and data up to and including and , or the older Impact Level (IL) 3. Where information attracts a high protective marking or IL, advice be sought from the and the .

Handling data on IT systems

This section covers how data be handled on IT systems, this includes both:

- Data in transit.
- Data at rest.

For the purposes of this guide, the term "sensitive" data or information refers to data or information which attracts a handling caveat of .

Ownership of information

All information is assigned an individual who has overall responsibility for the various handling aspects including:

- Registration.
- Labelling.
- Storage.
- Any transfers.
- Setting a retention period.
- Deleting, destroying or returning data and media.
- Ensuring that any applicable legal, regulatory or contractual obligations are adhered to.

This individual is the Information Asset Owner (IAO). The IAO ensure that information for which they are responsible for is appropriately handled, and where there is a business requirement to share it with a 3rd party, that it is shared in a safe and secure manner.

Electronic data transfer and storage

Data be stored only on managed accredited networks, with transfers onto remote access laptops or other mobile devices or media minimised. No sensitive data should be stored solely on non-networked devices or media unless specifically approved by the IAO.

Data in transit

The term "data in transit" covers all electronic moves or transfers of data from one IT system to another, where either the sender or the recipient system is an IT system. This includes the electronic movement of data using either a system-to-system connection such as CJSE, or removable media such as a USB mass storage device.

Secure network (system-to-system electronic transfer)

The preference for transferring data is to use a secure accredited government network whether that is a owner network (e.g. DISC, ONMI, Quantum or MINT) or the Government Secure Intranet (GSi).

As these networks can support data up to and including , a base level of assurance is provided. However, consideration will need to be given to the following factors to ascertain if any additional security controls are required:

- The amount of data being transferred.
- Frequency.
- Any "need-to-know" considerations.

Any additional controls be captured on the DMF (refer to the Data Movement Form). Advice should be obtained from the when required.

USB mass storage device

If using a secure network is not feasible, the next preferred option is to use an encrypted removable media, such as an approved USB mass storage device.

For more information, refer to the Removable Media guidance.

The type of device selected is normally dependant on the sensitivity of the data and the amount of data being transferred. Advice be sought from the on the best option to use when completing the DMF (refer to the Data Movement Form).

Optical media

The use of optical media (i.e. CD/DVD) is not recommended for data transfer.

Data at rest on -issued laptops

"Data at rest" is a term used to refer to all data in computer storage. This excludes data that is traversing a network, or temporarily residing in computer memory to be read or updated. The protection of data at rest is achieved by encrypting the hard disk. -issued laptops use an approved whole disk encryption product. This allows data to be safely stored.

Disposal and decommissioning

Sensitive data be kept for longer than is needed. The IAO check for compliance, including any mandatory retention period.

Physical media containing sensitive data be disposed of securely, even if that data is encrypted. The reason is that an attacker could potentially make unlimited attempts to crack the encryption used if the media comes into their possession.

Further information on disposal and decommissioning can be found in the Secure Disposal of IT Equipment guidance.

Information sharing

General principles

Where there is a business need to transfer sensitive data, it be appropriately secured or encrypted using an approved mechanism prior to electronic transmission or export to removable media devices.

Transferring sensitive data with the appropriate security controls may be achieved by:

- Transmission over a secure network that is accredited to carry such data, either in clear (where this has been formally approved by Information Assurance and the IAO), or encrypted.
- Transmission over an unprotected network, employing encryption of sufficient strength to mitigate any communication security risks identified.
- Physical transportation of storage media using encryption of sufficient strength to mitigate the security risks associated with the information being transferred in addition to the physical and procedural measures required to protect the media itself.

Note: Only the minimum amount of sensitive data necessary to meet the business requirement should be transferred and not the entire data set.

The sender ensure that any data shared can be adequately secured by the recipient. The sensitivity of data never be downgraded in order to send it over inadequately protected channels, or to send it to a recipient who does not have an appropriate facility to protect it after it arrives.

Sharing sensitive information

staff, including contractors and agency staff, make sure they observe the following measures when sharing sensitive information:

- Check that all recipients are authorised and cleared to receive sensitive information before sending it to them.
- Ensure that the confidentiality of the sensitive information is protected during transit, for example by encrypting the data.
- Ensure copies of sensitive information are not kept beyond when they are actually required, for example by keeping information "just in case" it might be needed in the future.

All staff avoid exposing sensitive data to unnecessary risks, in particular by observing all aspects of Acceptable Use.

Authorisation be sought from the IAO before sensitive information can be moved or shared with a 3rd party. The authorisation itself is captured within the Data Movement Form. the following sub-sections provide guidance on particular types of information sharing common across the , and to help you complete a DMF.

Internally within the

Information marked up to and including can be transferred in bulk within an IT system or domain such as DOM1, without additional controls required to preserve the confidentiality of that information.

Where information is transferred between IT systems or domains, additional controls might be required to:

- Ensure the information is routed correctly to preserve its confidentiality.
- Maintain the integrity of the data in transit to guard against inadvertent, accidental or deliberate modification.
- Ensure the exchange cannot be repudiated by either party, for example, be enabling proof of sending or proof of receipt.

Information transferred between two IT systems requires a completed and authorised Data Movement Form using one of the data in transit options.

Information sharing with another HMG department

Information shared with another government department be transferred to an assured system. This means the system be assured to the same level as the data being transferred. The transfer take place using one of the data in transit options. The preference is for information to be transferred using a secure network. However, for low frequency bulk transfers of data, approved removable media might be more suitable. A completed and authorised Data Movement Form is required.

Information sharing with external 3rd parties

Any transfer of sensitive data to a 3rd party, including sub-contractors or service providers, be authorised by the relevant IAO. An appropriate contract, Data Movement Form, and Non-disclosure Agreement (NDA) be in place prior to the transfer.

Where the information is , it be transferred to an assured system, assured to the same level as the data being transferred, provided by the external 3rd party, using one of the data in transit options.

Any transfer to a 3rd party be undertaken with appropriate security controls in place, using the guidance from this document, and seeking advice from the as required.

Sharing across an unsecured network

Sensitive data be encrypted prior to being transmitted over an unsecured network such as the Internet. The encrypted data may then be sent via file transfer or as an email attachment.

Ideally, both sender and recipient should check the integrity of data before and after transmission. This includes checking for malicious content, and for evidence of tampering during transit.

Using commercial encryption products for low sensitivity information

Where there is a business requirement to do so, sensitive information may be shared with a 3rd party using a commercial grade encryption product such as SecureZip. Further information on the use of SecureZip can be found in Using SecureZIP.

Note: File encryption does not protect the name of the file. This could reveal clues as to the nature and importance of the encrypted data. Encrypted files should be given innocuous names for transmission. If the data is contained in numerous small files, these should be collected together into a single archive ("zip") file. This archive should then be encrypted. Each file or archive should be sent separately, rather than attaching multiple encrypted files to a single email.

Sharing information higher than

Where there is a business requirement to share information classified higher than , advice be sought from the prior to completing a Data Movement Form.

Data Movement Form (DMF)

The Data Movement Form (DMF) is available here.

The purpose of the DMF is to ensure that the movement of information assets is secure, and in compliance with the .

Failure to fulfil or comply with the controls and measures identified within the DMF will lead to unnecessary risk or exposure for the , or the relevant Information Asset Owner (IAO), or the Senior Information Risk Owner (SIRO).

A DMF be completed, and approval received from the , for the following scenarios:

- Data is being moved or shared by using a physical storage device to transfer the information. An example is where you use a "memory stick", a USB drive, a storage array, or some other removable media. The DMF in this scenario focuses on the data being moved or shared.
- Data is being moved or shared by electronic (network) communication, where the movement is from an IT system to an external party. An example is using secure file transfer or approved email to transfer the information. The DMF in this scenario focuses on the data being moved or shared.
- An asset (a "data bearing asset") is being moved to, or transported by, an external party. This might be as a result of an office move, or because the asset is being decommissioned. The asset might contain or process information. Examples of data bearing assets include laptops, servers, multi-functional devices, and any other data bearing peripherals. The DMF in this scenario focuses on the asset being moved or transported, rather than the information that the asset might contain or process.

A DMF be submitted to the for information purposes, in the following scenarios:

- Data is being moved or shared by electronic (network) communication, where the movement is entirely within or between IT systems.
- Data is being moved in full compliance with the already-approved service design and operation specification and procedures.
- An asset (a "data bearing asset") is being moved but remains within the or its supplier-provided and -approved facilities at all times.

Note: In the informational scenarios, a DMF is only expected the first time a data movement or sharing takes place. Subsequent, repeat instances of the movement or sharing, do not require a re-submission of the DMF. For example, when setting up a backup process as part of an approved service design, a DMF is created and submitted to the for information purposes, but does not need to be re-created or re-submitted for each backup occurrence. If the implementation or process for the data movement or sharing changes, for example a new new backup technology or process is deployed, then a fresh informational DMF is required.

In any case of doubt, it is always advisable to complete a DMF and await approval or other feedback from the .

Using SecureZIP

SecureZip is a compression and encryption product which can be used to encrypt sensitive data for use in removable media and email based information transfers.

Note: SecureZip can produce "self-extracting" encrypted files that are executable programs which are likely to be blocked by network firewalls or email content checkers.

The general rules for transmitting a password to a recipient are:

- Never transfer the password with the encrypted file, or even over the same communication channel. Use an alternative method, for example if an encrypted file is sent by email, communicate the password or key via SMS text message, letter, fax or phone call.
- Transfer the encrypted data file first. Only send the password or key after the recipient has confirmed receipt of the file.
- Avoid detailing the purpose of a password when it is sent.
- Avoid re-using passwords and demonstrate good security discipline to 3rd parties by creating a completely new password or phrase for each transmission.

More guidance on password best practices is available.

Government Classification Scheme

The Government Security Classification (GSC) system has three levels: , , and .

The GSC was issued by the Cabinet Office in 2018: https://www.gov.uk/government/publications/government-security-classifications

This is the majority of information that is created or processed by the public sector.

> Includes routine business operations and services, some of which could have damaging consequences if lost, stolen, or published in the media, but which are not subject to a heightened threat profile.

This classification applies to the vast majority of government information including general administration, public safety, criminal justice, and law enforcement, and reflects the fact that reasonable measures need to be taken to look after it and to comply with relevant legislation such as the Data Protection Act, Freedom of Information Act, and Public Records Acts.

A limited amount of information is particularly sensitive, but still comes within if it is not subject to the threat sources for which is designed, even if its loss or compromise could have severely damaging consequences. The need to know principle be rigorously enforced for this information, particularly where it might be shared outside of a routine or well understood business process. There are very few activities where all related information or cases require the marking, though this might apply to assets previously marked as `CONFIDENTIAL`. Across a range of information assets which were previously normally marked as `PROTECT` or `RESTRICTED`, there might be individual cases/instances which are more sensitive (some of which might be marked `CONFIDENTIAL` on an individual basis). This more sensitive information is identified by adding ", and must therefore be marked ". This marking alerts users to the enhanced level of risk and that additional controls are required.

Very sensitive information that justifies heightened protective measures to defend against determined or highly capability threats.

> Where compromise might seriously damage military capabilities, international relations or the investigation of serious organised crime.

Use of only be used where there is a high impact and a sophisticated or determined threat (elements of serious and organised crime, and some state actors):

- Classified material received from Other Government Departments (OGDs) or agencies relating to national security and counter-terrorism.
- Intelligence and investigations relating to individuals of interests to security agencies.
- Information that might seriously damage security and intelligence operations.
- Information affecting the ability to investigate or prosecute serious or organised crime.
- Personal/case details where there is a specific threat to the life or liberty of an individual such as protected witness scheme records.

The concept of sophisticated or heightened threat doesn't only apply to those with a high technical (IT) attack capability, but might apply to criminals who have a developed capability to intimidate or coerce individuals. If disclosure of information might result in serious physical harm or put a life at risk because there is a real and highly capable threat present, the information be tightly controlled. become the default status for material just because of the type of case or potentially severe consequences such as murder trials, or where there is a threat to life. The threat capability also be present.

HMG's most sensitive information, requiring the highest levels of protection from the most serious threats.

> Where compromise might cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level. Any business area holding or expecting to hold information at this level contact the Departmental Security Officer to agree controls.

Applying the classification system

The following considerations apply:

- Staff and delivery partners are responsible for ensuring that all information is looked after with care, to enable the business to function as well as meeting privacy needs.
- The majority of and wider government information will fall into the tier; there is a significant step up to and which are essential for national security and the very highest threat areas.
- provides for a general and sufficient level of control of information (including for systems holding such information) which is not subject to heightened threat sources. Within this, there is flexibility to apply additional operational controls to reflect sensitivity.
- In most areas of activity at , staff should continue to follow existing business instructions and procedures for handling information that apply to those activities. Such instructions should include provisions for identifying and dealing with more sensitive cases.
- The 'Working with Official information' desk aid and handling rules should be referred to when receiving, handling or creating information in any format, which is not routine or covered by general processes or instructions.
- Material at does not require a marking to be applied, but must be protected in accordance with the handling rules and any local instructions. However, information assessed to be particularly sensitive must be marked , giving a clear warning that strict control of access and special handling apply (see below).
- Staff are expected to comply with local instructions and minimum controls, but need to exercise common sense in situations where applying a control is not possible or would seriously hinder effective business or safety. In all but the most urgent cases, seek approval from your manager or the Information Asset Owner before adopting lesser controls. Decisions must be risk based, and the assessment must be recorded at the earliest convenient opportunity.
- Existing material with former protective markings including `UNCLASSIFIED`, `PROTECT`, and `RESTRICTED` does not need to be retrospectively reclassified. See the transition note in this guidance.
- Descriptors, such as `PERSONAL` or `COMMERCIAL` are no longer used. In exceptional circumstances or where the recipient might not recognise the sensitivity of the information being sent, authors may include 'handling instructions' in a document or email to draw attention to particular requirements.
- The security officer for your part of the should be consulted to agree controls if you receive,handle or otherwise process any information at or .

Controls

At , any local instructions or operating procedures should continue to be followed. These should assist staff in identifying any cases that require the marking.

This guidance note and the desk aid entitled "Working with Official information" provide some general rules. You might also need to refer to local intranet pages or the handling rules if creating or processing any non-routine material.

Controls should be consistent with the minimum controls set out in the Handling Rules. These must be applied to all information within and are adequate for most information, providing defence against the sort of threats faced by a major company. These threats include, but are not limited to, 'hacktivists', single issue pressure groups, investigative journalists, competent individual hackers, potentially aggrieved participants or users of the justice system, and the majority of criminal individuals and groups.

Business areas or Information Asset Owners (IAOs) should review risks to their information, and ensure local procedures are in place, adopting additional controls where needed.

The Handling Rules document identifies additional considerations for some aspects of control. Business areas or IAOs might decide to adopt more robust controls in these areas, particularly for material marked or where information is moved, transmitted or otherwise communicated outside of the secure office environment.

Controls should be applied proportionately for information which would previously have been 'unclassified'. Such information still needs looking after if it is required for the job, but might not require controls designed to provide confidentiality.

If IAOs or staff are considering classifying any new assets or reclassifying any existing assets as or , they should consult their IA lead and security adviser, or with security in relation to technical threats, to determine whether a heightened threat might be present, and to agree necessary controls.

Marking of information

Marking is only needed for information which is , or . Classifications can be added to information in many different ways but the most important thing is that the marking is clearly visible to anyone using or receiving the information.

This could mean:

- Marking the top and bottom of documents, clearly, in `CAPITALS`, and `CENTRED` in the header and footer.
- Showing the marking in the subject line of emails:
  - Type at the start of the subject line, in `CAPITALS`.
  - Remember to consider whether material that is sensitive needs to be sent, and whether it is safe or appropriate to send if the recipient is outside a secure government network.
  - You must not email anything at or above.
- Marking the front of folders or binders:
  - Apply clearly in a prominent position in `CAPITALS`.
  - Apply the highest classification of any of the contents.

Material that needs marking must be transmitted securely. The classification of contents must not be visible on an external envelope sent by post or courier.

Transition to the classification system

For information bearing the 'old' markings, the following guidance should be followed to ensure appropriate handling. Unless there are specific instructions to the contrary, staff are expected to maintain current levels of control and use existing IT systems on which information is currently held or processed.

The old protective markings do not automatically read across, particularly at `CONFIDENTIAL`.

- All material up to and including `RESTRICTED` becomes .
- Much material at `CONFIDENTIAL` becomes , but some might become .
- Only a limited amount of material at `RESTRICTED` needs marking as .
- `CONFIDENTIAL` material moving into is likely to require marking as .

Old marking	New classification	Examples
`UNCLASSIFIED` or not protectively marked.	Treat as (unmarked). Where controls prevent otherwise safe sharing of non-sensitive information, IAOs have some discretion to relax controls, provided any relaxations are specific to their assets and have no wider risk consequences, such as for the security of IT assets and government network code of connection.	Public notices and leaflets, published information, information that doesn't contain personal data or other sensitive content, and training materials.
`PROTECT`.	If information relates to general administration, treat as (unmarked). Where used for personal data, maintain existing controls. Individual case records containing particularly sensitive content need to be marked , though these instances may already be marked `RESTRICTED` or `CONFIDENTIAL`.	Documents containing personal data such as personnel records, citizen or offender case records, and general administration not intended for publication.
`RESTRICTED`.	If it relates to general administration, there should be a presumption that it can be treated as (unmarked).	General administration, policy documents, commercial documents, or case records.
	You need to consider whether the subject matter is particularly sensitive and there is a need to rigorously enforce access controls, in which case material may additionally require handling or marking as . Anything with this level of sensitivity might already have agreed handling constraints. If in doubt, discuss with the Information Asset Owner.	Particularly sensitive case records, contentious policy drafts and advice, and sensitive negotiations.

Old marking	New classification	Examples
CONFIDENTIAL hard copy previously received from another Department.	Check with the author or originating Department. The presumption should be to treat as and continue with current handling controls, unless there is a clear national security aspect or it relates to protected witnesses, in which case treat as . If you want to reproduce content in an electronic document, check the classification with the author or originating Department. See the note after the table.	
CONFIDENTIAL electronic copy received by secure government network or held on stand-alone system used for CONFIDENTIAL.	Continue to observe the operating instructions for the system you are using. Continue to use the secure government network for any reply, and use the marking applied by the original author. Otherwise, adopt controls for . See the note after the table.	
.	Continue to treat as , subject to any formal review of the classification of the information assets involved in the particular area of activity. If hard copy, treat as and log, store, move and dispose of accordingly. If held on a stand-alone system currently rated at , treat as and observe the operating controls for the system.	Material relating to national security or counter-terrorism, and some protected witnesses.

Note: Electronic records marked CONFIDENTIAL should not be processed or saved on the existing standard networks such as DOM1 or Quantum, or on electronic document management systems unless or until the originator or Information Asset Owner has issued revised guidance allowing the information to be handled at , including , and the system has been rated to hold material at , with any additional access controls, or the system reclassified as .

Information classification, handling and security guide

All employees interact with information, and are responsible for its protection. Information security must be considered during the process of designing, maintaining, and securing the 's IT systems that are used to process information.

However, not all information warrants the strictest levels of protection. This is why information classification is so important to the – to ensure that the department can focus its security efforts on its most sensitive information. Information security must be proportionate to the security classification of the information, and must be considered throughout the information lifecycle to maintain its confidentiality, integrity, and availability.

Classifying information

The three information security classifications the uses are , , and . This follows the .

Each information security classification has a minimum set of security measures associated with it that need to be applied. These security measures might change, depending on the information lifecycle stage.

Classification	Description
	All information related to routine business, operations, and services. If this information is lost, stolen, or published, it could have damaging consequences, but is not subject to a heightened threat profile. For regular, unsupervised access to information, someone would be expected to have achieved Baseline Personnel Security Standard (BPSS) assessment.
	Very sensitive information that requires protection against highly sophisticated, well-resourced, and determined threat actors. For example, where compromise could seriously damage military capabilities, international relations, or the investigation of a serious crime. For regular, unsupervised access to information, someone would be expected to have passed National Security Vetting Security Check (SC) clearance. In exceptional circumstances, someone with BPSS might be granted occasional supervised access to UK assets, or be required to work in areas where or information might be overheard.
	Exceptionally sensitive information that directly supports, or threatens, the national security of the UK or its allies, and requires extremely high assurance of protection from all threats.

Securing the 's information must be done with a combination of information security measures:

Type of Measure	Description
`PERSONNEL`	Personnel should be aware of their security responsibilities and in turn acquire security clearances and undertake training to support the 's information security objectives.
`PHYSICAL`	Tangible measures that prevent unauthorised access to physical areas, systems, or assets.
`TECHNICAL`	Hardware or software mechanisms that protect information and IT assets.

It is important to understand that security classification is determined by the level of risk in case of loss or unauthorised access, and not by the type of information.

It is the responsibility of the Data Owner to classify the data.

- Most production data is information. Within this, some production data might be classified as information.
- Most personal data is information. Within this, some personal data might be classified as information if it meets the risk threshold defined.

The following table sets out the definitions for each security classification, as well as whether it is necessary to explicitly "mark" a piece of information with its classification type.

Classification	Definition	Marking
	All information related to routine public sector business, operations and services.	

Classification	Definition	Marking
	Almost all personal information falls within the classification.	
	is not a separate security classification. It should be used to reinforce the "need to know" principle, beyond the baseline for .	data does not need to be marked except where , and must be marked .
	Very sensitive information that requires protection against highly sophisticated, well-resourced and determined threat actors, for example serious and organised crime.	Must be marked
	Exceptionally sensitive information that directly supports (or threatens) the national security of the UK or its allies and requires extremely high assurance of protection from all threats.	Must be marked

Additional information on how to manage information is described in the Information Asset Management Policy.

Information security classification may change throughout the information lifecycle. It is important to apply appropriate security classifications and continually evaluate them.

The consequences of not classifying information correctly are outlined as follows:

- Applying too high a marking can inhibit business operations, such as collaboration, and lead to unnecessary and expensive protective controls being applied.
- Applying too low a marking may result in inappropriate controls, and may put sensitive assets at greater risk of compromise.
- Incorrect disposal can lead to unauthorised access to information. Disposal of information should be done using approved processes, equipment or service providers.

and

All of the 's information is, at a minimum, information. It is very likely that the information you create and use in your day-to-day job is information.

Examples include:

- Routine emails you send to your colleagues.
- Information posted on the intranet.
- Supplier contracts.
- Information and data you use to build a database, such as database secrets, record types, and field types.
- Most production data.
- Most non-production data.

means that the 's typical security measures are regarded as sufficient.

whilst not a formal classification, should be used sparingly, so that its effectiveness is not weakened. This is especially important when you consider that is already well-protected.

Use when you want to remind users to be careful when handling information. This asks them to use extra care, beyond what is expected for the baseline classification.

The threshold for classifying information as information is very high. It is unlikely that you will encounter information in your day-to-day job.

information should not usually be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is , contact the immediately.

To help decide whether some information should be classified as , ask yourself a simple question:

> If a hacker gained unauthorised access to the information, could it compromise the security or prosperity of the country?

The answer is most likely "No". In that case, you should consider using the classification.

If the threshold for classifying information as is very high, the threshold for classifying information as is extremely high. It is very unlikely that you will encounter information in your day-to-day job.

information should not be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is , contact the immediately.

To help decide whether some information should be classified as , ask yourself a simple question:

> If a hacker gained unauthorised access to the information, would it directly and immediately threaten the national security of the country?

The answer is most likely "No". In that case, you should consider using the or classification, as appropriate.

Reclassification examples

When deciding whether it is appropriate or desirable to reclassify information, a useful model is to consider what audience might get value from accessing the information. For example, if a hostile country might want the information, then the information might well be best classified as . Alternatively, a reclassification decision might be required as a result of changing threat advice from intelligence agencies.

Example 1

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as , with the handling caveat.

A user wishes to share a copy of the report "as-is" with their team. They cannot remove the handling caveat without prior discussion and agreement from the asset owner.

Example 2

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as , with the handling caveat.

A user wishes to share a subset of the report with their team. In particular, the report is substantially re-worked to remove all the private information. The user becomes the owner of this new asset. They are responsible for this new asset. They can decide that the handling caveat is not required.

The original report retains its classification and handling caveat.

Example 3

An asset owner creates a report. The report contains information about plans to handle a pandemic. The asset owner decides that the report should be classified as , with the handling caveat.

A user reviews the report. They realise that the information could potentially compromise the security or prosperity of the country. They decide to increase the classification of the report, and treat it as . They discuss this decision with the asset owner, so that the original report is correctly reclassified.

Handling and securing information

The is the most comprehensive guide on the security measures necessary for each of the three security classifications, including measures related to the following:

- Personnel (administrative) security.
- Physical security.
- Technical (information security).

The following sections set out the minimum measures you need to consider when handling and securing information within the different levels of classification.

Handling and securing and information

Type	Measure	Example
PERSONNEL	Make sure all staff including contractors undergo baseline security clearance checks.	A contractor working with the Security Team must undergo a baseline background check (i.e. BPSS check) at minimum. Refer to Security Vetting Guidance.
PHYSICAL	Make sure that you lock your screen before you leave your desk.	
	When working in an unsecured area, for example when working remotely, think about whether unauthorised people might be able to eavesdrop on your conversations, or look over your shoulder at your screen.	
	The has additional requirements when moving assets which can be found in the .	A software developer working from a flatshare should take calls in private, and use headphones and a privacy screen.
	Transferring information from one location to another requires planning and preparation, including a risk assessment. More information on this is available in the , and from your manager.	A technical architect working on the requirements for a new platform should lock their laptop before leaving their desk.
TECHNICAL	Protect information "at rest" by using appropriate encryption.	In the development of a new cloud-hosted solution, the following criteria should be considered: remote access connections and sessions are encrypted using an appropriate VPN; information stored "at rest" on end user devices and the cloud is encrypted; information in transit between the end user and the cloud service, such as payment services, is encrypted; and the cloud service used is a service.

Type	Measure	Example
	Appropriate encryption is also necessary when protecting information in transit.	When using any services over the PSN, make sure you fully read the agreements that you make with the service provider for details and definitions about the data you use or transfer using the service, to ensure you understand the risks to compliance, confidentiality, integrity, and availability.
	services can be used for information.	
	You must not use removable media such as an USB memory stick unless it is unavoidable. When you have to use one, it must be issued, encrypted so that the effects of losing it are minimised, and the data erased securely after use.	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the for further guidance.

Handling and securing information

Type	Measure	Example
`PERSONNEL`	Make sure employees and contractors undergo Security Check (SC).	A contractor working with the Security Team must have at least SC before being allowed to access information.
`PHYSICAL`	Consider using multiple layers of security to protect information. information should be held on a secure computer network which is physically isolated from unsecured networks and the internet.	Imagine you are moving locations for a server used to host information. The encrypted server is secured in a locked and monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after relevant parties, including the data owner, line manager, and the system owner, have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two SC-cleared individuals, for example, employees of a specialised commercial courier company.
	Transferring information from one location to another requires planning and preparation, including the completion of a Risk Assessment and the use of SC-cleared personnel. More information on this is available in the and from your manager.	

Type	Measure	Example
`TECHNICAL`	information at rest should be protected with very strong encryption. Contact the for more information.	
	Care should be taken to ensure that information in transit is only shared with defined recipient users through assured shared infrastructure or using very strong encryption.	
	information should be processed on IT systems which have been approved for the threat model. Advice on what commercial IT systems meet this requirement is available from the .	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the for further guidance.

Handling and securing information

Type	Measure	Example
`PERSONNEL`	Ensure employees and contractors undergo Developed Vetting (DV) security clearance checks.	A contractor working with the Security Team should have at least DV clearance before being allowed to access information.
`PHYSICAL`	Handling and storing information requires exceptional planning, monitoring, and record-keeping.	Imagine you are moving locations for a server used to host information. The encrypted server is secured in a locked and continuously monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after you, your manager, and senior managers have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two DV-cleared individuals, for example, employees of a specialised commercial courier company. When it happens, local police may need to be informed and involved in providing an additional layer of security.
	Working remotely with is not permitted due to the extreme sensitivity of the information.	

Type	Measure	Example
	Transferring information from one location to another requires even greater planning and preparation than for information, including the completion of a Risk Assessment by senior management and the use of DV-cleared personnel. More information on this is available in the and from your manager.	
TECHNICAL	When physical security measures cannot be used, information at rest should be protected with extremely strong encryption. Contact the in these circumstances.	
	Care should be taken to ensure that information in transit is only shared with defined recipient users through accredited shared infrastructure or using extremely strong encryption.	
	information should be processed on IT systems which have been approved the threat model. Advice on what commercial IT systems meet this requirement is available from the .	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the for further guidance.

Note: For further information on statutory disclosures and transfer to national archives, please refer to the .

Information Classification and Handling Policy

This document provides the core set of IT security principles and expectations on the handling and classification of information on IT systems.

The stores and processes a wide variety of information, some of which attracts an HMG protective marking or contains personal information. The has a duty to protect all the information stored and processed on its IT systems.

This policy outlines the Information Classification and Handling Policy for all information held on IT systems.

Scope

This policy covers all staff (including contractors and agency staff) who use IT systems.

The overarching policy on information classification and handling is maintained by Security. This document only contains IT specific policies which are in addition to the overarching policy.

The overarching policy can be found here.

All Users **must be** made aware of the Information Classification and Handling Policy, and provided with security awareness training which covers this policy.

All Users **must be** provided with refresher security awareness training which covers this policy every 12 months.

Inventory of assets

All information assets need be identified and have a nominated asset owner, to help ensure that the appropriate protection of these assets is maintained.

Examples of what an information asset constitutes are:

- Databases and data files.
- System documentation.
- User manuals, training material, operational or support procedures.
- Security documentation such as RMADS or disaster recovery plans.
- Archived backup data.

The list of information assets and associated Information Assets Owners is coordinated and maintained by individual business groups, where the responsibility resides with the business group SIRO.

All business groups **must maintain** a list of information assets, their associated named Information Asset Owner (IAO), and which IT systems they reside on.

Note: Some information assets might not be held on IT systems.

Deriving a classification

At the , all information assets are assessed against HMG guidance on business impact, and HMG guidance on the protection of personal data. This assessment is used to select the appropriate classification from the Government Security Classification scheme.

All information assets stored or processed on IT systems **must be** assessed for a Business Impact Level, where an impact level for the Confidentiality, Integrity and Availability for each asset is derived.

The Asset Owner is responsible for determining the classification that applies to an asset.

All users are responsible for applying the appropriate classification to information assets created or handled on an IT system, where a pre-existing classification does not exist.

Note: As outlined in the IT Security Policy, all data and assets must have IT security controls designed and implemented to protect Confidentiality, Integrity, and Availability.

Further information on the criteria and derivation for classification can be found at: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/.

Application of Government classification

The Government classification scheme defines how information should be labelled and handled. Output from IT systems containing information that is classified must carry classification labels where it is or higher. This includes, but is not limited to, printed reports, removable media, electronic messages (such as email) and file transfers.

All IT hardware and removable media assets **must** be labelled with the highest classification from among each of the individual information assets stored or processed on it.

Note: This classification might be reduced if sufficient security controls are applied, for example whole disk encryption, and if there is agreement with the system assurer or .

All output from an IT system **must** be given the classification of the highest of each of the individual information assets contained within that output.

Where applying a classification label is not feasible, an alternative method **must be** agreed with the system assurer or .

Further information on the criteria and derivation for classification can be found at: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/.

Information handling on IT systems

The policy for handling classified material applies to all IT assets and all outputs from an IT system.

Media handling

Removable media

Any systems or removable storage media used for work purposes must be encrypted to security standards. Security encryption is a mandatory government measure, and one of the most important methods we have to protect information.

What is 'removable' media?

Laptops and USB memory sticks are the 's most commonly used items of removable media. Removable storage media covers items available to users, such as USB memory sticks, writeable CDs/DVDs, floppy discs, and external hard drives.

Strictly speaking, magnetic tapes are also removable storage media, but it would be very unusual for the average user to have access to or to use magnetic tapes for business purposes.

security guidance specifies that USB memory sticks and other user-removable media should not be used to store departmental data. Only in exceptional circumstances, and where there is compelling business justification, should -approved USB sticks with device encryption be used.

USB memory sticks

This guidance is intended to ensure that data remains secure, and to mitigate the potential impact of lost data sticks.

1. You must only connect approved external removable storage media to systems.
2. Connecting non-approved memory sticks is a breach of security guidelines, and could result in disciplinary action.
3. If there is a genuine business requirement to save, retrieve or transfer data via removable media, fill in one of:

   - Removable media business case form
   - Data Movement form

   Additional guidance information is available about the Data Movement form. When the form is ready, send it to: .
4. Each request is evaluated by Operational Security, with a view to recommending the safest and most appropriate method to contain risk of loss.
5. Normally, you'll get a response within 5 working days.
6. Requests to use a memory stick or other removable media will normally only be granted when there is no other practical alternative. Where approval is granted. only encrypted memory sticks or other removable devices provided by the are allowed. Use of memory sticks or other removable devices will be subject to stringent conditions, and permitted only after user training.

If you need further assistance or information about this process, ask.

How do I know if my laptop, or USB stick, is encrypted?

All equipment provided through the 's recognised central procurement systems are encrypted and protected to security standards. You must use processes to obtain any equipment used for business purposes, including mobile computing devices and removable media.

What's expected of you

Keeping information safe is everyone's responsibility. Anyone using portable computing equipment must take particular care to safeguard the equipment and the information stored on it. Failure to do so may result in disciplinary procedures.

Secure disposal of IT equipment

The and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, both physical and virtual. These resources are procured and managed though suppliers, who are normally responsible for the secure disposal of the resources when no longer used.

However, there are also other physical and virtual resources across the estate which might have been procured and managed locally. It is crucial that they are disposed of in a secure manner, to prevent data being leaked.

Note: When disposing of or equipment, materials, or resources, you contact security:

Secure disposal of IT - physical and on-premise

This document is the guidance covering disposal of physical and on-premise media and data. It is intended to ensure that the confidentiality and integrity of data is maintained when physical hardware is decommissioned.

Physical Media and Associated Data

The and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, including photocopiers and printers, data centre hard and tape drives, desktop computers, laptops, USB memory sticks, and generic mobile devices. Some equipment might be the responsibility of a supplier to decommission and dispose of it safely and securely. Check asset tags or similar identifiers to determine and validate responsibility.

However, other devices across the estate might have been procured and managed locally. They be disposed of securely, to prevent information from being "leaked".

Approved organisations

For help to arrange secure disposal by an approved organisation, contact .

and on Secure Disposal

The and give critical guidance on the secure sanitisation of storage media here and here, respectively, specifically regarding disposal and destruction of media, and the data contained within it.

The situations when sanitising data is required are:

- Re-use.
- Repair.
- Disposal; sanitising unwanted media and its associated data whilst it is controlled by the and before it is passed outside the .
- Destruction; destroying the media, and hence data it contains, onsite or offsite.

Determining data deletion and destruction methods

To determine the data disposal and the media's destruction method, based on the type of equipment and its security classification, use the following table.

The table contains two columns, called "Data deletion method" and "Destruction method", which are defined as:

Data deletion method

Covers assets if they remain within the , and have not reached end of life. For example, the device can be re-used or reallocated to a different user, or repurposed for a different function.

Destruction method

Covers assets that have reached end of life, and need to be physically destroyed onsite or offsite.

Note: If the data is encrypted, then only the key needs to be deleted or erased, and the table does not need to be followed.

If the table does not cover your exact requirement, contact .

Note: When disposing of or equipment or materials, always contact .

Equipment or asset type	Data deletion method	Destruction method
Flash (USB)	Delete the data, or erase using manufacturer instructions.	Destroy using commercially available disintegration equipment, to produce particles of a maximum of 6 mm in any direction.
Hard disk drive. This includes data centre disk drives.	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Break the platters into at least four pieces. This can be carried out either manually or by using a commercially available destruction product suitable for use with hard disks. Alternatively, apply a lower level degauss (refer to the explanation after this table), and then apply a destructive procedure that prevents the disk from turning. For example, punch holes into the platters, or twist or bend them.
Magnetic tapes and floppy disks This includes data centre tape drives.	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Destroy using a commercially available shredder that meets a recognised international destruction standard. Particles of tape should be no larger than 6 x 15 mm. Alternatively, apply a lower level degauss and then cut the tape to no larger than 20 mm in any direction.
Optical media	Data deletion is not possible.	Shred or disintegrate using equipment that meets a recognised international destruction standard. Particles should be no larger than 6 mm in any direction.
Monitors	Overwrite on-board storage by displaying non-sensitive data on the screen for a few minutes before powering off. If a monitor screen has legible "burn-in" of sensitive information it be re-sold or donated.	Monitors can be disposed of by: (1) Returning the product to the manufacturer who align to formal waste disposal responsibilities, or (2) taking the item to a professional waste disposal facility, or (3) reselling or donating to a non-profit organisation, once basic sanitation procedures have been performed. Ensure there is no "burn-in" of sensitive information, and that the device has not reached its end of life. If the end of life monitor contains mercury, it is considered hazardous waste and its disposal align to WEEE 2013 Regulations using specialist methods such as disassembly to remove the mercury containing backlights for specialist treatment and the separation of the remaining material streams.

Note: A lower level degauss is a process using specialised equipment to erase data totally, by eliminating the unwanted magnetic field (information) stored on tape and disk media.

Owners of the data storage devices are responsible for procuring services that meet the necessary destruction outcomes as described previously.

Wherever possible and appropriate, managers should pool together equipment with that of local colleagues to share service costs.

Data destruction verification

As part of the physical media or data destruction by the or its suppliers, validation of destruction be carried out. This is to ensure that data handling processes align with the Asset Management Lifecycle policies. This includes:

1. The or supplier scans the hard drive or physical media asset tags or barcodes.
2. The or supplier carries out data destruction (as per the previous table).
3. The or supplier confirms hard drive or physical media data destruction by providing reasonable proof. This can include:
    a. Providing an inventory of physical media in their possession.
    b. Reconciliation carried out on the physical media scanned/received matching the physical media destroyed.
    c. A witness in attendance to sign a destruction certificate that is be stored in a secure space or network share.

Note: An alternative to the previous steps is to use a leading enterprise erasure tool that provides a certificate aligned to NIST 800-88 Guidelines for Media Sanitization. Such a tool verifies:

1. When the physical media was destroyed.
2. That verification was performed.

If you are based in a London HQ site the Accommodation Team coordinates bulk secure disposal; please contact them in the first instance.

Note: All destruction certificates and destroyed assets be supplied to the hardware team to update CMDB. This can be done using the technical portal to "Bulk upload CIs - update", or alternatively by emailing the details to: MoJITAssetManagementTeam@justice.gov.uk.

Transporting data between sites securely

If you have any concerns about moving items between sites securely, contact .

Guidance on the transportation of secure data is located in the CPNI guidance: "10. Transport of sensitive items".

The previous guidance is also referenced in the CAS Sanitisation Service Requirement, under section "MIT001 – Keep items secure during transportation" on page 9.

Working securely with paper documents and files

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.PPR.xxx**, where **xxx** is a unique ID number.

Audience

This guidance complements the overall security policy.

This guidance applies to all employees, contractors, partners, and service providers, including those on co-located sites and sites owned by other public bodies. This includes employees of other organisations who are based in, or work at, occupied premises.

POL.PPR.001: Agencies and arm's length bodies (ALBs) comply with this corporate framework but establish their own arrangements tailored to operational needs and supplement this framework with local policy or guidance for any business-specific risk.

Objective

The requires employees and contractors to get into the habit of looking after the information that they work with, whether it is on paper or stored electronically, in the same way that they would take care of their personal valuables.

Scope and Definition

This guidance helps you understand the risks involved in working with, sharing, and moving paper documents both inside and outside the office. It covers any information that relates to the business of the , its stakeholders, or partners, where the information has been printed out or written down on paper.

Note: This guidance applies also to the contents of personal information systems, such as notebooks.

This guidance outlines the basic principles of working securely with paper documents and files.

Context

All information is valuable. There is a requirement to protect everything that relates to the department's business, including information provided by others.

Note: The protection requirement applies to all information, not just information that is covered by the Data Protection Act or classified under the government-wide security classification system.

There are different rules for managing and protecting various kinds of paper-based information. You know how to:

- Identify the correct security level for the information you work with.
- Handle the information according to the relevant rules.

Responsibilities

All employees, contractors, partners, service providers and employees of other organisations who are on premises or co-located sites remain accountable for the security, health,and safety of themselves, colleagues, and the protection of departmental assets.

Policy statements

Identifying the correct security level

The uses the government-wide security classification system to indicate the level of security that the various types of information require. The different classifications are based upon the harm that would be caused if controls were breached.

POL.PPR.002: Within the classification, material does not normally need to have the classification written on it. However, particularly sensitive information be marked with the handling caveat if it requires more robust access and handling controls to prevent more damaging consequences from disclosure.

POL.PPR.003: Information handled in the might not always have a visible classification marking. If any file contains material with a marking, then the cover of the file be marked with the highest level of any of the contents.

To identify the right security level for information, think about:

- How sensitive that information is.
- Whether it contains personal data that could be used to identify individuals.
- What the consequences might be if the information was compromised or misused.
- Whether the information is likely to be under threat from anyone with a high intercept capability. If so, the information might require marking at a higher classification than .

If you are in any doubt, ask your line manager or contact .

Allocating security levels and marking

POL.PPR.004: If you are generating original information, you apply the standard rules to decide which classification to use. Do not set security levels higher than necessary. Set the classification that is appropriate at the time. Classification can be altered later if circumstances change, such as when material is no longer embargoed or has been released intentionally for consultation.

POL.PPR.005: For material at or higher classifications, the classification be written in capitals at the top and bottom of each page of the document. You use the header and footer facility if creating electronically, and include page numbers by using the format `Page x of y`. You only create documents at classification levels higher than on approved IT systems. Files and documents be marked according to the most sensitive piece of information included.

Data Protection Act

If the information in the documents or files can be used to identify living individuals, or could identify living individuals when used in conjunction with other material, then the information is covered by the Data Protection Act (DPA). The Act covers not only information such as name, address, and date of birth, but also expressions of opinion about or intentions towards an individual.

POL.PPR.006: Paper-based information that is covered by the DPA be managed according to the general principles of working securely with paper documents and files set out here.

Handling paper-based information in the office

Think carefully before leaving papers unattended on desks, in the same way that you would avoid leaving your own personal correspondence – or even a purse or wallet – in plain view.

The has a clear desk policy that is intended to ensure information is seen only by people who 'need to know' it.

This means:

- Not leaving documents or files on a desk when not being used.
- Locking documents or files in a secure cabinet when you leave the office.

Failure to follow this policy could expose files and papers to the risk of being seen during the working day by other staff, or visitors to the office and, out of hours, by guards and cleaners. Even apparently non-sensitive information should be looked after. Putting papers away also protects them from damage from fire, smoke, or water.

There are different controls regarding how the various levels of classified information are secured. Refer to the Information classification, handling and security guide for more information.

Taking documents and files out of the office

Occasionally, you might need to take information outside premises. Examples might be when you are working from home, or moving between buildings. At such times, it is likely that you'll be carrying valuable information within documents, paper files and personal notebooks.

POL.PPR.007: Always check first whether it is really necessary to take documents out of the office. If it is essential to do so, you get permission from your line management, especially if the information includes:

- Personal information, including anything that relates to an identifiable individual or individuals, such as staff, stakeholders, partners, or customers.
- Material marked .

POL.PPR.008: You get permission from a head of division, or from a member of the Senior Civil Service (SCS) if the information is marked at a level higher than . Removal or relocation of information marked at a level higher than be noted and recorded on a register, and a record kept of when the material is logged back in.

POL.PPR.009: If you are carrying papers out of the office, you protect them against accidental loss such as an accident or distraction, causing you to drop or misplace them.

POL.PPR.010: Ideally, carry papers in an unmarked case. For papers marked or higher, or when using public transport, you use a lockable case.

POL.PPR.011: For short journeys, such as on foot, and where you are not stopping or using public transport, it is acceptable to carry papers in a plain envelope, marked only with your name and office address.

POL.PPR.012: If carrying papers to a meeting at a different location, you allow sensitive details to be visible. The reason is that they could be photographed by a journalist.

POL.PPR.012.001: Papers be stapled together or otherwise secured in a package. This is to limit dispersal if the carrying case or envelope becomes damaged or opened.

POL.PPR.013: Cases or envelopes have the minimum details necessary on the outside to assure safe return of the item, if lost, without having to be opened to reveal the contents.

POL.PPR.014: Documents be left unattended in public places or in an unattended car. Care be taken if you are reading protectively marked information in public places where you might be overlooked, such as a train, or where it might be difficult to retrieve a document if you lost hold of it, for example if you dropped it, or it was blown away.

If you are taking papers home, ensure that they are not readily accessible to other members of your household. Take precautions to minimise their loss. If the papers would normally be locked away in the office, try to do the same at home.

Sending documents

Options for sending documents are covered in the Sending Information guidance note.

Disposing of paper information

offices have bins or bags that are specifically intended for secure waste disposal of documents or files, including:

- Personal information that relates to an identifiable individual or individuals.
- Sensitive information that be disclosed.
- Any material bearing a visible classification marking.

POL.PPR.015: You read and follow the secure waste disposal guidance on the Intranet before disposing of any document or files.

POL.PPR.016: Before disposing of information, you check whether it should be retained on a file, and whether it is covered by a 'retention schedule'. The can advise on this.

Long-term storage

The has arrangements for the secure long-term storage of paper documents and files. If you want to keep paper-based information, but no longer need to regular access to it, refer to the information on the Intranet regarding keeping, deleting, and disclosing information. The can provide additional guidance.

What to do if you think there has been a security breach

POL.PPR.017: If you suspect that the security of the information you work with has been compromised in any way, you report it immediately.

Note: A security breach does not have to involve the actual loss of information. The potential loss of information also counts. For example, if a security cabinet has been left unsecured, there may be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

POL.PPR.018: The level of risk and potential impact to assets, and, most importantly, physical harm to our people and the public, determines the controls to be applied and the degree of assurance required. The ensure a baseline of physical security measures are in place at each site, and receive annual assurance that measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, such as in response to a security incident or change in the Government Response Level.

POL.PPR.019: The implementation of all security measures be able to provide evidence that the selection was been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the , and .

The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards is subject to annual review or more frequently if warranted.

Physical security advice

Physical security advice can be obtained by contacting .

Access control

User responsibilities

Protecting social media accounts

Hostile attacks on Social Media accounts pose a serious threat to the and its reputation. When attacks happen, they quickly become headline news, and can happen to any account, anywhere in the world.

Two types of attacks are common:

- Attempts to render the account useless by 'bombarding' it with messages.
- Attempts to 'take over' the account.

Steps we can all take to protect ourselves

Ensure our passwords are secure

Passwords are the main protection on our accounts, hence ensuring they are secure is vital. The NCSC has produced guidance on making secure passwords - the summary of which is that picking three random words to make a password (for example `RainingWalrusTeacup`) is a good policy for securing Social Media accounts.

Check your email details are up-to-date

Most of the time, the first indication you'll have that something is wrong is when an email is sent to you. This could be to let you know that someone is attempting to log into your account, or that someone is trying to reset your password, or more worryingly, that a new device has logged into your account. Hence it is important that you ensure that your email details are up-to-date, and that your email is secure.

Enable Two Factor Authentication

Two Factor Authentication (2FA) involves requiring a random code to be entered before being logged in. These codes are either sent to the user via SMS or email, or generated every 30 seconds by an app or device the user has which relies on a seed key provided by the service. That seed can then be shared amongst a team, allowing for multiple owners or contributors.

If at all possible, SMS generation should be avoided, as it is theoretically possible for phone numbers to be taken over through various attacks, as well as meaning that only one person can receive the code, which isn't ideal if a team is working on a single account.

If you're using email, then it can be sent to a group account, which also allows for multiple owners or contributors - but it's important to ensure that the email is also protected by 2FA.

If you have a spare 10 minutes, watch this video for an excellent explanation of how 2FA works and why it's important to have it enabled.

Click the links for details on how to activate 2FA for Facebook, Twitter and Instagram.

Only use trusted third-party applications

In addition to the official applications, there are many tools and third-party applications that might be used to work with social media accounts.

Some of these tools provide useful extra facilities, such as 'scheduled' posts, or helping you post one message to several different social media channels.

The problem is that you have to give your account details to these tools so that they can post to your account.

This is potentially very dangerous:

- An application might post messages on your behalf, that you do not agree with or are unacceptable.
- An application might store or share your account details.

Only use applications that are trusted and approved for use with your social media accounts. For help with this, contact Cyber Security.

Remove 'unused' applications

People tend not to be very good at removing old or rarely used applications. Older applications should be checked regularly to find out if there are any updates.

A good habit is to check your applications once a month or so, and consider:

- Do you still use the application? If not, remove it.
- Whether there is an update available for the application? If so, install it.

As well as increasing safety, removing unused applications frees up storage space on your system.

Check your privacy settings

The whole point of a social media account is to share information. But that doesn't mean you want to share *everything*.

When you first create a social media account, you are normally asked to decide on the privacy settings. These control how much information you share, and who you share it with.

Typical settings that affect privacy include:

- General information about you.
- Your Profile information and photo.
- When you were last active.
- Any status updates.
- Whether you have read direct messages ("Read Receipts").
- Whether others can add you to their groups, possibly without your knowledge or agreement.

But it's very easy to forget to check the settings, from time-to-time, to make sure they are still correct.

A good habit is to check your account privacy settings once a month or so. Information on privacy settings is available for the main social media environments:

- Facebook
- Instagram
- Twitter
- WhatsApp

For example, in WhatsApp, to prevent someone adding you a group without your knowledge, change your settings: **Settings** > **Account** > **Privacy** > **Groups** > **My Contacts**. This change means that only people you know (your contacts) can add you to a group.

Limit access to your accounts

You might be tempted to share access to your social media account, for example if you want to have postings regularly, even while you are away.

Avoid sharing access to your social media account. It's easy to forget who the details are shared with. It's also possible that postings might be made on your behalf that you don't agree with, or are not acceptable.

Any social media accounts that do need to be shared will have proper access controls in place. You should never need to share your account details for work purposes.

If you need more help on this, contact your Line Manager or Cyber Security.

Don't click on suspicious links

Unfortunately, social media postings are a common way of sending you links to malware or other problem material. Postings might also be used to send you 'phishing' attacks.

In the same way that you should be careful with any links or attachments sent to you using email, you should also be suspicious of links or attachments sent to you though social media. This applies to both general postings and messages sent directly to you ('Direct Messages').

For more information, read this article on the Intranet.

What to do if your account is bombarded

Remember that these attacks are short lived

Due to the amount of organisation and effort required to coordinate such an attack, they do not last long, and like an intense inferno, will soon burn themselves out.

Do not respond to the attack

These attacks are designed to attack the person controlling the account as well as the agency itself. By only responding to messages not involved in the attack - especially those trying to share positive messages, the attackers will run out of interest far sooner than if you engage them. If they are posting harmful or threatening messages, report the accounts.

In a single sentence - "don't feed the trolls".

Feel free to walk away

Dealing with these attacks can be emotionally draining; even just reading the messages can have a far greater impact on you than you realise. Take breaks in the event of an attack, even if it's hard to - consider going for a walk to force yourself away.

System and application access control

Password Managers

guidance makes clear that you should have different passwords for different services. These passwords must be complex.

But how do you remember all these different passwords?

The simplest way is to use a Password Manager. If you have lots of different, and complex, passwords for all your accounts, using a password manager makes life much easier.

This article provides guidance on using password managers within the .

Password managers and vaults

A password manager stores sensitive information in an encrypted form. Password managers are sometimes called password vaults.

In the , password managers are tools that you might use for your personal accounts. Password vaults are tools that a team of people might use to look after details for shared accounts.

Password vaults usually have extra strong access controls, such as hardware tokens.

Here, we use password manager and 'password vault interchangeably, except when stated otherwise.

When to use a password manager or a password vault

The following table shows when you might use a password manager or vault:

Scenario	Tool	Notes
Single user, personal accounts	Password manager	For accounts that only you use, or have access to, then you would probably store the details in a password manager. An example would be storing the username and password for your work email account; only you should have access.
Multiple users, shared accounts	Password manager or password vault	Some accounts might be shared between a group of users. For example, a team might need to know the password for an encrypted document. If the access required is for a sensitive or operational system, then a more heavily protected tool such as a password vault might be appropriate.
System access, no human use	Password vault	Some systems need to 'talk' directly to other systems. No humans are involved in the conversation. The passwords protecting these communications can - and should - be extremely complex. A strongly secured password vault would be ideal for this purpose.

Best practices

The NCSC is very clear:

- "Should I use a password manager? Yes. Password managers are a good thing."

This is helpful for us in the , as much of our IT Policy and guidance derives from NCSC best practices.

Good password managers

A password manager should never store passwords in an unencrypted form. This means that keeping a list of passwords in a simple text file using Notepad would be A Bad Thing.

Good password managers encrypt the passwords in a file using strong encryption. It shouldn't matter where you store the encrypted file. Storing the list "in the cloud" lets your password manager access the data from any device. This is useful if you are logging in from a laptop, or a mobile device. Storing the passwords locally means the password manager works even when offline.

A good password manager will have:

- Strong encryption for the list of passwords.
- Network access for encrypted lists stored in the cloud.
- A dedicated app but also a pure web browser method for working with your password list.
- A tool to generate passwords of varying complexity.
- The ability to fill in login pages.

What password manager to use

In the NCSC article, they are very careful not to identify or recommend a password manager. This ... caution ... is the reason why we don't say much about password managers within the guidance.

There are several password managers used within the . KeePass and 1Password are probably the most popular for personal or team passwords. To determine whether a particular password manager is suitable for work usage, check the General app guidance.

Example password vaults would be Hashicorp Vault, Kubernetes Secrets or AWS Key Management.

For individual use, have a look at 1Password. Try it out. When you decide on a password manager, request approval from your line manager to install and use it: "I'm planning to install and use XYZ to manage my passwords, is that OK?".

Refer also to the Using 1Passwords guidance.

Passwords

This article provides guidance on passwords and Personal Identification Numbers (PINs) within the . It helps you protect IT systems by telling you about choosing and using passwords and PINs. Whenever you encounter the word "system" here, it applies to:

- Hardware, such as laptops, PCs, servers, mobile devices, and any IT equipment.
- Software, such as the Operating System, or applications installed on hardware, or mobile device applications (apps).
- Services, such as remote databases or cloud-based tools like Slack.

This guidance is for all users.

Note: Except where stated, the guidance in this article applies to both passwords and PINs.

General best practices

Note: This section applies to passwords and PINs.

You share your password or account details with anyone, unless you have documented approval to share from your Line Manager or higher senior manager.

If a system or another person provides you with a password, change it before doing any work on that system. Examples of 'single-use' passwords include:

- Your own account on a work-provided laptop.
- A shared account for accessing a data analytics service.

- All supplier or vendor supplied accounts.

You change a password whenever:

- There has been a security incident involving your account or password. For example, someone guessed your password, or you used it on another account.
- There was a security incident with the service that you access using the password. For example, if someone broke into the system that provides the service you use.
- Your line manager or other authorised person tells you to do so.

When required to change a password, you do so as soon as possible. If you don't change the password soon enough, you might be locked out of your account automatically. The following table shows the maximum time allowed:

Type of system	Maximum time to change a password
Single-user systems, such as laptops	1 week
All other systems	1 day

Best password practices for everyone

Note: This section applies to passwords only, not PINs.

The password guidance follows NCSC guidance. The NCSC recommends a simpler approach to passwords. Some agencies or bodies might have specific requirements or variations. Check your team Intranet or ask your Line Manager for more information.

Follow the CyberAware advice to generate your passwords. Always use a separate and unique password for each account or service.

The most important points to remember are that passwords should be:

- At least 8 characters long.
- No more than 128 characters long.
- Not obvious.
- Not a dictionary word. A combination of dictionary words might be suitable, such as "`CorrectHorseBatteryStaple`".
- Unique for each account or service.

Best PIN practices for everyone

Note: This section applies to PINs only, not passwords.

Some devices, especially mobile devices, only support numerical passwords, or Personal Identification Numbers (PINs).

If the device supports passwords, then passwords be used rather than PINs.

If the device supports only PINs, you :

- Always use a separate and unique PIN for each account or service.
- Ensure the PIN is at least 4 characters long.
- Avoid using obvious PINs, such as `1234`.
- Avoid using repeating digits in the PIN, for example `0000` or `9999`.

App-based password protection for files

Some applications - including Microsoft Office tools such as Word, Excel, and Powerpoint - provide mechanisms for protecting files. A password controls whether someone can open, or edit, a file.

While these app-based password protection mechanisms are better than nothing, there are three good reasons for avoiding them if possible.

1. You depend on the application to provide and maintain strong password protection. If the password implementation fails, or has a weakness, you might not know about it. This means that you might think your information is protected, when in fact it is at risk.
2. It is tempting to use a standard password for protecting a file within the app, so that other people can share and work with the file. Changing the password becomes "inconvenient". The result is that many versions of the data file are all protected with the same password. Also, if anyone has ever been given the password to access the file, they will always be able to access the file.
3. If you forget the app-based password, there might not be a recovery process available to you.

For these reasons, advice is that you use password tools within an app to protect data files that are processed by the app. For example, you use the password tools with Microsoft Word, Excel, or Powerpoint, to protect information within files. Instead, either:

1. Store the data files in a shared but secure area, such as the SharePoint storage facility.
2. Use separate encryption tools to protect data files, separate from the app that works with the data files.

Of these two options, storing data files in a shared but secure area is strongly preferred. The reason is that you can add, modify, or revoke access permissions to the storage area easily.

If you have no choice, and have to use app-based password protection, ensure that the same password is not used indefinitely for a data file. You use a different password for:

- Each major version of a data file, for example version 2.x is different to version 3.x.
- Any data file where the password is more than three months old.

Note: This advice is a specific exception to the general guidance, that you do not normally need to change passwords.

Password expiry

You don't have to change a password because it is old. The reason is that time-expiry of passwords is an ...outdated and ineffective practice.

Some current or legacy systems don't allow passwords that follow guidance. For example, some mobile devices, laptop hard drive encryption tools, or older computers might not be able to support a mix of character types. For such systems, choose passwords that are as close as possible to guidance.

Password managers

Use a password manager to help you keep track of your passwords.

These are tools that help you create, use, and manage your passwords. A useful overview is available here.

As passwords become more complex, and you need to look after more of them, it becomes increasingly necessary to use a password manager. For example, development teams in Digital & Technology use 1Password.

You still need to remember one password. This is the password that gets you into the manager application. Once you have access, the application works like a simple database, storing all the passwords associated with your various accounts and services. Some managers have extra features, such as password generators. Some managers can even automatically fill-in username and password fields for you when during log in.

The password manager database is often stored in the cloud so that you can use it anywhere. The database is encrypted, so only you can open it. That's why your single password key is so important. Without it, you can never get access to the password database again.

Using a password manager for your account and service details is recommended.

You can find additional useful information about password manager tools here.

Default passwords

Change all default passwords when a new, modified, or replacement system arrives. Complete the changes before making the system available for any work.

When preparing devices or services for first use, system developers or system administrators configure the default password on the device or service so that it can be used once only. The “first use” of a password forces the user to change the password before the device or service can be used.

Password access attempts

If a password is ever entered incorrectly, a count starts. After at most 10 (ten) consecutive failed attempts at using the correct password, access to the account or system is locked. A successful use of the password resets the count to zero again.

Password reset

If a password lock occurs, a reset is necessary. This requires action by the system administrator or the . The process should be like issuing the password for the first time. Other account details are not changed during the reset. This helps avoid losing any work. Checks ensure that an attacker cannot use the password reset process.

Blocking bad passwords

You should not try and use obvious passwords. Attempts to do so will be blocked.

Single-use passwords

Some passwords are 'one time' or single-use. Administrators and developers use these to grant access to a service for the first time. After using the password once, the user immediately change the password.

Single-use passwords are time limited. If they are not used within a specific time after generation, they become invalid.

The following table shows the valid lifetime of a single-use password:

Type of system	Lifetime of a single-use password
Single-user systems, such as laptops	1 week
All other systems	1 day

Using 1Password

What is 1Password?

1Password is an online password management tool that we make available to you to help you create, store and share passwords. Using it means you no longer need to remember dozens of passwords, just a single primary password. It keeps all your website logins protected, helps with creating new 'strong' passwords and password sharing when required.

1Password is available as a browser extension for popular browsers, as well as a full software suite (for use outside of browsers) for Microsoft Windows and Apple macOS.

1Password securely saves your credentials in your own 'Vault' and then offers to autofill those credentials the next time you need them.

The has the Business tier of 1Password.

Who should use it?

Currently, 1Password accounts can be requested by service or operations teams that have a need for shared passwords.

How to get it

Contact the to request access.

Make sure you include in your message:

- which team you're in
- your role in your team

- why you need access

What it can be used for

1Password can be used for sharing passwords within a team, when individual named accounts cannot be created in the service. A good example is running a shared Twitter account.

Note: If you have a business need for a shared Twitter account, consider using a more enterprise-orientated tool for social media posting, such as TweetDeck or Hootsuite. You need formal approval to use tools like these.

Personal use

You use your 1Password account to store personal non-work information as it is a work account belonging to the . You may lose access if you change role. You will lose access entirely if you leave the .

Operations Engineering cannot routinely access the contents of vaults but can reset accounts to gain access if there is a good reason to do so.

What it shouldn't be used for

1Password be used for storing personal passwords, or for storing documents. Use existing approved services such as Office 365 or for storing documents.

You use 1Password for 'secrets' that belong to systems, only credentials to be used by humans.

How to use it

Getting started

You will be sent an email to your work email account inviting you to create your account. 1Password have 'getting started' guides on their website.

Creating your primary password

You need to create a primary password - this is the only password you'll need to remember.

It be at least 14 characters long (the longer the better).

You can choose to make it pronounceable and memorable (passphrase) such as `CyberSecurityRules!` or `Sup3rD00p3rc0Mp3X!`, as long as you're comfortable remembering it and won't need to write it down.

There are password guidance standards here.

Your primary password be unique and you use it anywhere else (including a similar version, for example, by simply adding numbers to the end)

Multi-Factor Authentication

You setup multi-factor authentication (MFA, sometimes known as 2FA) for your account.

1Password has a guide on setting up MFA.

If you don't have an -issued work smartphone you may use a personal device for MFA.

Sharing passwords

To share a password, create a Vault.

You make sure the credentials you're sharing are only available to the people who need to access them for work. It is your responsibility to remove items or people from vaults when access to the credential(s) is no longer required.

You share your 1Password main password with anyone, even your line manager or security.

Using it overseas

Taking a device (such as personal smartphone) that has 1Password installed counts as travelling overseas with information.

The has existing policies on travelling abroad on the intranet, which require various approvals before travel.

It may be simpler to 'log out' of the 1Password applications or enable Travel Mode to remove vaults from your devices. These can be reinstated when you return to the UK.

Keeping 1Password update to date

Like all software, it is important to keep the software up to date (sometimes known as 'patching'). 1Password software generally self-updates to the latest version by itself, however make sure you approve or apply any updates if 1Password asks you to.

Need help?

If you need help *installing* 1Password contact the relevant .

If you need help using 1Password such as getting access to vaults or resetting your primary password as you have forgotten it, contact s.

Physical and environmental security

Equipment

Clear screen and desk

There are many helpful policies and best practices that improve safety and security.

Note: In addition to this advice in this document, you should review and follow the guidance in the remote working guidance, for example thinking before you print.

Clear screen

Users comply with the following:

- equipment be left logged on when unattended. Users ensure that password-protected screensavers are activated when any equipment is left unattended.
- Computer screens be angled away from the view of unauthorised persons.
- Computer security locks be set to activate when there is no activity for a short pre-determined period of time. This timeout be set to 5 minutes, by default. The screen lock be manually activated when required.
- Computer security locks require passwords to be re-entered to reactivate the computer.
- Desktops and laptops be shutdown if you expect to be away from them for more than half an hour.
- Users log off or lock their computers when they leave the room.

A best practice is to keep your screen 'desk top' tidy:

- Avoid leaving files on your desk top where the name might attract attention. For example, having a file on your desk top called `MyPasswords.docx` is a bad idea, for several reasons!
- Avoid having files or information labelled displayed or stored on your desk top.

Clear desk

Users comply with the following:

- Where possible, paper and computer media be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, particularly outside working hours.
- Where lockable safes, filing cabinets, drawers, cupboards, or similar secure storage areas are not available, doors be locked if rooms are left unattended. At the end of each session all and information be removed from the work place and stored in a locked area.
- When handling documents security follow the requirements laid down in the Government Classification Scheme (GCS).
- or information, when printed, be cleared from printers immediately.

Think before you print.

It is good practice to lock all rooms and office areas when they are not in use.

Information left on desks is also more likely to be damaged or destroyed in a disaster such as fire or flood.

Equipment Reassignment Guide

Introduction

This guide describes how to reassign equipment. It applies to laptops, mobile phones or other issued equipment. Reassignment is from one user to another.

Who is this for?

This guidance applies to:

1. **Technical users**: these are in-house Digital and Technology staff. They are are responsible for implementing equipment controls. The controls apply throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
2. **Service Providers**: defined as any other business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, and storing data) for, or on behalf of the .
3. **General users**: all other staff working for the .

"All users" means General users, Technical users, and Service Providers.

Returning Equipment

When a project completes, or a colleague leaves or moves to a new role, equipment no longer required be returned. The Line Manager (LM) is responsible for using the Service Catalogue to request a return of the item. The equipment might then become available for use by other employees. It might not be cost-effective to consider reusing or reassigning the equipment. Possible reasons include:

- Older technology that might have been heavily used.
- The likelihood of operating problems and failures.
- Lack of support, updates, or patches.
- Slower performance.

As a result, it might be preferable to use a new machine, rather than repurposing a reassigned device. The decision depends on the expected use of the reassigned device.

The LM is responsible for ensuring a review of the equipment. This is to ensure that sensitive data be lost by erasing the contents of the device. This task be delegated to the team member most familiar with the data. The LM remains responsible. Any sensitive data identified be copied and relocated to a secure location. This can be the Teams facility or to Sharepoint. This happen before the device is made ready for reuse or destroyed.

Any IT equipment which is no longer needed, or has reached its "end of life" have its data securely deleted and confirmed to be unreadable and unrecoverable before destruction, redistribution, or reuse of the equipment.

Equipment Reassignment

Equipment be passed from one user to another without being formally reassigned.

Equipment be completely "cleaned" to an "as-new" state before it is reused or reassigned. This means that all storage media in the device be fully erased. A sufficiently secure method for "wiping" equipment be used. Deleting visible files, emptying files from the "Recycle Bin" of a computer, or reformatting a device are not considered sufficiently secure methods for wiping equipment. The reason is that data recovery software might be used by a new owner to "undelete" files or "unformat" a device.

To erase data securely, use appropriate "data-shredding" tools for the media being erased. Typically, these tools do not simply delete data, they overwrite it multiple times. The overwriting erases all traces of the data, making it almost impossible for any retrieval. Another option is to re-encrypt the device using a different password, then delete the data to free up space.

Equipment reassignment be recorded by the LM in the appropriate asset register.

Equipment that cannot be reused

If IT assets are no longer needed by the , and cannot be securely wiped, then the equipment need to be destroyed physically. More information can be found at Secure disposal of IT equipment

Regrettably, for security reasons, redundant IT equipment be donated to charities, schools, or similar organisations.

Leased equipment

Managers ensure that any equipment that is leased has a data destruction clause written into the contract. Under such an arrangement, the supplier ensure that data is wiped when it is returned.

Laptops

The guidance applies to all staff.

Related information

Lost devices or other IT security incidents on page 114

Storing data on laptops

If you need to store data on your computer you should always remember to move it into:

1. Your local Electronic Document and Record Management (EDRM) system.
2. An shared drive.
3. Your -provided 'home' drive.

Do this as soon as you can next connect to the network.

Where data should be saved when using a laptop

It is best to avoid saving any data on a laptop hard drive. However, if you absolutely must, you should always remember to copy or move the data to the network as soon as you next can connect to it, either via secure remote access or by direct connection.

In order to avoid potential data loss, save data in:

1. Your local Electronic Document and Record Management (EDRM) system.
2. An shared drive.
3. Your -provided 'home' drive.

There is a better chance of recovering lost data if you have saved it to the network, as data stored on the network is backed up daily.

The impact of hard drive failures

Hard drive failures can lead to the irrecoverable loss of data. Any data loss can have security implications for the , and a significant impact on:

- Our business opportunities.
- Our reputation.
- Our ability to deliver services to the public.

If you experience any issues with your laptop or IT service, ask for help.

For more information about the main security issues that are likely to affect remote and mobile workers, refer to the remote working guide.

How to reset your password

To reset your password, you will need to contact the #unique_328. They will carry out checks to confirm your identity. This might include asking your line manager or court manager to confirm your identity, by sending an email to the . Once your identity is confirmed, your password will be reset and you will quickly regain access to your laptop.

Locking and shutdown

The has made a commitment towards sustainable IT. The intentions are:

- To reduce overall power consumption for the by switching off machines and saving energy.
- To reduce the 's overall carbon footprint.

Shutting down a desktop computer

- Close all applications.
- Shut down the computer by clicking the 'Start' button at the bottom left hand corner of the screen. Next, click 'Shut Down'.
- A pop-up box will appear with a drop-down box. Select 'Shut Down' and click 'OK'. After a short delay, your computer will automatically shut down.
- Switch off your monitor screen.

The benefits

By switching off our computers at the end of each working day, we are contributing towards being energy efficient and environmentally friendly. We are all responsible for our own Carbon Footprint. So, please switch off your PC monitor along with your desktop computer at the end of each working day. In addition, please switch off any other PC monitors if you notice they too have been left on overnight.

Dealing with issues preventing you from switching off your computer

If there are any issues preventing you from switching off your desktop computer overnight, then please raise this with the #unique_333 immediately as there could be an underlying fault that needs resolving.

If you require any further information regarding this policy, ask for help.

Locking your computer sessions

Access to most computer systems is controlled by a user name and password. If you have the correct information, you are able to 'log in' or 'log on'. The user name identifies the user as a valid user of the system and the password authenticates that the user is who they say they are.

You are responsible for what you do with an system or service. You might be held responsible for any actions carried out using your user name and password. You must therefore not allow any one else to do work on any system using your user name and password. If you leave your computer logged on when you are away from it, it might be possible for sensitive information held on the computer system to be used, read, changed, printed or copied by someone not authorised to access it.

If you are leaving your computer unattended for a short period of time, 'lock' the computer by activating the password protected screen saver or similar 'locking' facility. A simple and quick way to lock a Windows computer is:

1. To LOCK - press the Windows key and L key, at the same time.
2. To UNLOCK - press the Ctrl, Alt and Delete keys, at the same time, then log in as normal.

A simple and quick way to lock a Mac computer is:

1. To LOCK - press the Ctrl, Cmd and Q keys, at the same time.
2. To UNLOCK - move the mouse or press any key, then log in as normal.

Laptops

All laptops have hard disk encryption installed. This protects the entire contents of a laptop's hard disk drive to prevent any data stored locally from being accessed in the event the laptop is either lost or stolen.

Laptop incidents

Investigations into security incidents indicate that a common reason for problems is where the correct security procedures are not being followed. For example, laptops are being left logged on overnight.

This is not good security practice.

If a device is lost or stolen whilst the machine is in locked mode, the data on the machine is more vulnerable to a potential security breach.

Leaving the laptop in premises is not sufficient to guarantee the equipment's security. Laptop losses do sometimes occur within offices. There is a greater risk of data loss when a laptop is left partially logged on overnight, so you should always fully log off the laptop at the end of your working day.

Laptop security

- Switch off the machine completely at the end of each usage.
- Do not attach the password to the machine or keep the password with the machine.

If you need further assistance or information about this process, ask for help.

Policies for MacBook Users

Any User of an -supplied MacBook must ensure they comply with this policy, to ensure that security is not compromised when using these devices.

These Policies are supplementary to the GOV.UK and Enterprise policies, procedures and guidance.

If you are unsure about any of the requirements or content, ask for help.

Policies

- You must not share your login details or password with anyone under any circumstances.
- You must change your password if you suspect it has been compromised, or if instructed to do so by your line manager or other authorised individual.
- You must not attempt to access any other person's data unless you have been authorised to do so.
- You must only collaborate with authorised personnel.
- Get help if you are subjected to any security incident, or suspect you might be.
- You must logoff or lock your computer when leaving it unattended.
- You must keep your Digital& Technology equipment close to you and in sight at all times when in public areas.

Top things to remember

You are responsible and accountable for the security of your equipment at all times.

If you don't think you should do something, you probably shouldn't. If in doubt, always seek advice.

Operations security

Protection from malware

Ransomware

Ransomware is a type of malicious software created or used by cyber criminals. It prevents people or businesses from accessing their own data. The software takes hold of the data, holding it "hostage", until a ransom payment is made to release it.

Preventing Ransomware from taking hold of information

- Store all your information in official systems. This is general best practice, and also minimises the risk of the data being accessed by the hackers.
- Use a secure antivirus and firewall software. All official systems have these installed as standard.
- Use a trustworthy VPN when accessing public networks through wifi, for example when working remotely in a coffee shop. All official systems have a suitable VPN installed as standard.
- Ensure your laptop computer is updated regularly. All official systems do this for you automatically, as standard.
- Use multi-factor authentication (MFA) methods. Most systems support MFA, but you might have to enable it yourself.
- Do not provide any personal information to unknown contacts.
- Avoid insecure apps or websites.

Things to look out for if you suspect you have become victim to a ransomware attack

- Unable to open documents.
- Suspicious file names. Files encrypted by ransomware tend to end with `.crypted` or `.cryptor`, rather than the more typical names such as `.docx`, `.pdf`, or `.jpeg`.
- An unrecognised pop-up screen prevents access to your computer.

What to do if you think a ransomware attack is affecting your system

In the event of a ransomware attack, or if you have suspicions one may be taking place, the first thing to do is to contact your local .

With your help, the IT team attempt to determine which systems have been impacted, and can isolate them immediately. You might be asked to disconnect all your devices from the network or wifi connection, to prevent a further spread of attacks throughout the business.

Control of operational software

Guidance for using Open Internet Tools

This information applies to all staff and contractors who work for the .

This guidance gives you:

- An overview of Open Internet Tools (OIT).
- A quick checklist to help you decide if you can use an OIT.
- Reasons why you might, or might not, want to use an OIT.
- Things you must think about when using an OIT, such as data protection.
- Information on who to contact if you would like help or advice.

Note: To access some of the links in this guide you'll need to be connected to the Intranet.

Overview

Open Internet Tools (OITs) are applications or services from suppliers outside the . They often have the following characteristics:

- they are general purpose. This means they are not specific to the . Other organisations can use them
- they are accessed using the Internet, usually through a web browser. This means that if you have Internet access, you are able to connect to the tools
- they have a basic 'free-to-use' version. This means that you are able to use some or all the capabilities, but with some constraints. For example, an online word-processor might limit you to 5 documents in your account
- they have one or more 'paid for' versions. By paying for the tool, you unlock some or all the constraints

Quick checklist

To help you decide if you can use an OIT to work on an task, consider the following questions:

- is the task information subject to specific rules or requirements in your part of the ?
- is the task information classified as anything other than or?
- does the task information include any data identifiable as being about someone?
- is this the first time anyone has used the tool for business?
- does the tool need access to your account or other data you can access? For example, does it ask to use your Google or Microsoft Office account?
- does the tool install a web-browser extension?
- is the tool a plug-in for existing OITs we use, such as Slack, Confluence, or Jira?
- could there be damaging consequences if the task information you work with using the tool is:
  - lost
  - stolen
  - published in the media
- are you prevented from exporting all the data from the tool?
- are you prevented from deleting all the data from the tool when you finish working on the task?

If the answer to *any* of these questions is "Yes", you might not be able to use the OIT.

When you have all the answers, request formal approval to use the OIT from your Line Manager. Do this *before* using the OIT.

Why OITs are an opportunity

OITs offer some significant advantages for you and the , including:

- enabling you to work the way you want to, more effectively
- usually cheaper than buying or building and supporting a dedicated tool
- no need to build or support the tool
- good use of open standards, such as file formats
- reduced need to have specific hardware or software on computers
- rapid patching to address security issues
- easy updates and deployment of new features
- a large pool of help and support
- easy access, whenever you have a network connection
- increasing availability of some or all capabilities when disconnected from the network

Why OITs are a risk

OITs also pose some threats or risks, including:

- dependency on the tool and supplier
- security of access to the tool
- security of information stored within or processed by the tool
- potential difficulty of enhancing or customising the tool for -specific requirements

But as long you consider the threats or risks, and address them, OITs provide many benefits for you and the .

Summary

With careful use, OITs help you to work more effectively and efficiently. Think about them as serious and preferable options for performing tasks.

Using OITs

This guidance helps you:

- understand the conditions or constraints that apply to a tool, or a task performed using a tool
- identify and address threats or risks posed by a new tool

Privacy and personal information

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Don't use OITs for storing personal data until you have addressed the need to get consent first. Check if using the OIT might need an update to existing privacy policies or notices. Don't use OITs if unlawful disclosure of the information they process might cause damage or distress.

Data protection legislation might also limit *where* you can process personal data. An OIT should have a privacy statement that describes where it stores or processes data. Be ready to contact the OIT provider for more information about this aspect of their service.

Be sure you can fulfil your data protection responsibilities when using an OIT. It might be helpful to complete a Privacy Impact Assessment (PIA).

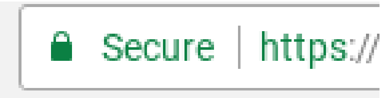
Complying with personal information requirements can be complex. Don't hesitate to ask for advice:

Classification and security

An OIT can only store or process information classified at level.

Think about the information you work with. What would happen if you lost it, or it's stolen, or published in the media? Suppose the information was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is "No", then it's probably OK to use OITs to store or send that information.

Think also about information moving across the Internet. The data might be safe within the and in an approved OIT. But what about the connection between the two? Sending information might involve insecure networks. Be aware of the security implications. Check that enough suitable security measures are in place to protect the information. For example, check for encryption of network connections using SSL/TLS. A simple way to do this is to look for the secure connection indicator in your web browser:



You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is Principle 2 of the Government Security Classifications. The trusts you to work with information. In the same way, you're trusted to make a reasoned judgement about whether it's safe to use an OIT.

Useful help for deciding what is OK is in existing social media guidance. While it's more about how to act online, the principles are helpful for OITs.

Remember that it is impossible to delete information after it's released in public.

For more information about IT Security, look on the Intranet here.

Storage and data retention

Laws and regulations make the and its employees responsible for managing information. Some examples include:

- the Freedom of Information Act

- the Data Protection Act and General Data Protection Regulation
- the Public Records Acts

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate systems helps us, because:

- we can provide evidence about decisions
- we understand the information held, and where to find it
- we can transfer records to The National Archives

Always store information in systems. If you use an OIT, make sure the key information is also stored in an appropriate system. Guidance on what you must keep is available. At regular and convenient intervals, transfer the information to an appropriate system. Do the same when you finish the work. Don't forget to remove any redundant information from the OIT.

Most OITs let you export your data. You can then store it on an appropriate system. Sometimes it's easier to copy and paste text into a new document. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

For more guidance, read the Information Management Policy. There is also help on responding to requests for information.

Service and support

OITs are often intuitive and reliable. But that doesn't mean they are always available and always work as you expect. The can't provide technical support or ensure service availability for them. Always have another way of working if the OIT is not available for some reason or for any length of time. In other words, don't let an OIT become business critical.

Check the OIT usage agreement to find out more about the service and support available.

Note: The cannot provide technical support for OITs.

Common OITs

There are already many OITs used across the . Permission to use an OIT might vary, depending on where you work in the . For example, some teams must not access or use some OITs, for security or operational reasons.

Note: Check with your Line Manager if you want to use an OIT for your work, *before* you use it.

Getting help

For further help about aspects of using OITs within the , contact:

Subject	Contact
Classification and Security	Cyber Security team
Storage and Data Retention	Departmental Library & Records Management Services (DLRMS)
Information Assurance	Compliance and Information Assurance Branch
Personal Data	Disclosure Team

Communications security

Information transfer

Bluetooth

This guidance helps you use Bluetooth enabled devices and peripheral devices.

Related information

Personal devices on page 26

Overview

Bluetooth is a very short range wifi technology. In everyday terms, Bluetooth devices can 'talk to each other' if they are very close, for example in the same room. This makes Bluetooth really good for wireless devices, for example a telephone headset, or a mouse or keyboard.

Bluetooth works by 'pairing' devices. This makes it quick and simple to use. The problem is that Bluetooth, and the pairing process, is not very secure. This means that attackers might get unauthenticated access to devices. As an example, an attacker 'listening' to the Bluetooth connection between a computer and a keyboard could possibly intercept passwords or other sensitive information as the details are typed on the keyboard.

This guidance tells you more about the view of Bluetooth, from a security perspective. It also gives you hints and tips on how to use Bluetooth more safely.

The aim is to help you maintain the Confidentiality, Integrity and Availability of data, applications and services. The results should be that:

- the information you access is not compromised
- you can connect devices using Bluetooth, safely
- you are aware of the problems around Bluetooth, and can take the necessary safety precautions

Note: Remember that there might be local rules that apply regarding the use of Bluetooth devices. A good example is in Prisons, where use of Bluetooth would not be available by default. Ensure that you check with local requirements.

Accessibility

Some types of Bluetooth devices are not allowed, by default. However, where there is a good reason for requiring a Bluetooth device, such as for Accessibility reasons, then a request for an exception to use the device will be treated sympathetically and permitted wherever possible.

Bluetooth devices and risks

Examples of Bluetooth devices, and whether they might be used for business purposes, are as follows:

Bluetooth device	Suitable for work purposes (Y/N)
Keyboards	Y
Mouse	Y
Telephone headsets	Y
Headphones	Y
Earbuds	Y
Trackpads	N - but exception possible for Accessibility reasons
External speakers	Y - but be aware of other people or devices nearby that might be listening

Bluetooth device	Suitable for work purposes (Y/N)
Gaming joysticks and controllers	N - but exception possible for Accessibility reasons
Laptops	Y - for -issued devices
Hearing aids	Y
Watches and Fitness bands	N
Smart TVs	N - requires authorisation
Storage devices (similar to USB 'thumb' drives)	N
Internet-of-things 'Smart speakers'	N
Connected vehicles	N - Connected vehicles are effectively Bluetooth-connected storage devices.

A Bluetooth device might be at risk from any of the following:

- Eavesdropping
- Unauthorised access
- Message modification
- Denial of service
- Data exfiltration
- Insecure data transmission
- Phishing

An example of a Bluetooth problem is 'Bluetooth marketing'. As you walk around with your mobile phone, it is continuously looking for Bluetooth devices and wifi access points. It does this to help with accurate location tracking. But other devices can also find your mobile phone. These devices might report tracking information about where you were at any time. This guidance will help you understand more about the problem, and suggest things you can do to reduce the risks.

Connected vehicles

Connected vehicles are effectively Bluetooth-connected storage devices. They are considered personal devices for the purposes of this guidance, regardless of whether they are owned, leased or rented.

Automatic transfer of contact information and calendar events might happen during the pairing process. The resulting transferred data is accessible to any third party who subsequently pairs their mobile device to the vehicle.

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. Transferred information might not be immediately visible or accessible, but this is not the same as deleting the information from the vehicle.

For these reasons, devices be paired with Bluetooth-enabled vehicles.

Best practices for using Bluetooth

Before using a Bluetooth device in a work context, consider the following:

- What is the business case for using the Bluetooth device?
- What data might be or will be access through, or using, the Bluetooth device?
- Does the Bluetooth device have the latest patches and fixes applied - where possible?
- Was the Bluetooth device purchased from a reputable vendor?
- Does the Bluetooth device require a PIN code or similar before connecting?
- Are the Bluetooth devices 'discoverable'?
- Have you connected to any other 'public' Bluetooth devices?
- Are all the devices password protected?
- Might someone be able to find out what Bluetooth devices you are using?

- Is the material you are working with or higher?

The best way to ensure your Bluetooth device is as up-to-date as possible is to apply all patches and fixes for all hardware devices as soon as you can.

Bluetooth is a very cheap and simple technology. This means that it is often included in extremely cheap devices; often these use old versions of technology or are not provided with patches and fixes. The best thing is to obtain any Bluetooth devices from reputable vendors, so that it is more likely the device will be supported and maintained correctly.

Many Bluetooth devices try and make connection as easy as possible by enabling 'Direct Connection'. This often means that you only need to 'find' a Bluetooth device on your 'phone or laptop, then click once for a connection to be established. While very easy, this is not safe, because those same direct connections can also happen automatically, 'behind the scenes', without you being aware. If possible, ensure that a Bluetooth connection is allowed only when a PIN or password is supplied. This reduces the risk of 'hidden' Bluetooth connections.

Some Bluetooth devices allow you to choose whether they are 'discoverable'. For example, on Android 'phones, you can go to the `Settings -> Connected devices -> Connection preferences -> Bluetooth visibility` or similar. The best advice is to change the Bluetooth settings to not discoverable if you can. Only make the device discoverable when you need to connect to a trusted device.

At regular intervals, check to find out what Bluetooth devices are 'known' to your devices. Remove any you don't recognise.

When in public places, make sure you only connect to known devices. Always ensure you are in a secure and safe location such as home, office, or a known isolated place before switching on your Bluetooth.

If someone can find what Bluetooth devices you have, or are using, they might try and use one of their device to intercept or monitor the connection. Try to keep Bluetooth devices out of sight so that no-one knows which ones you might actually be using. Even the bright blue light Bluetooth devices illuminate when they are connected might draw unwanted attention.

Generally speaking, Bluetooth devices do not present extra problems when working with material. However, the whole point of Bluetooth is to enable and simplify communications, so you need to be extra careful when using Bluetooth devices while working on or higher material.

Email

Overview

This document provides you with guidance for safe and secure use of email within the .

In general, always use email in an acceptable way.

In particular:

- Never circulate messages or material that contains obscene, profane, inflammatory, threatening, harassing (racially, sexually or otherwise), and disruptive, or otherwise offensive language.
- Don't use email or other messaging systems for trivial debates or exchanges with an individual or group of people.
- Don't use email or other messaging systems for anything other than appropriate business purposes.
- Don't make statements that defame, slander or lower the reputation of the , any person or organisation.
- Don't forward email chain letters to your contacts. Instead, report them to .
- Be aware of unsuitable attachments, for example video clips, images, or executable files. email automatically filters many unapproved attachment types, particularly those that can contain executable files. Emails containing those attachments are likely to be quarantined and not delivered.
- Avoid excessive use of email, and sending email to large numbers of recipients. Ask yourself if it really makes sense to "Reply All"?
- Any recipients in the "To" or "Cc" fields can retrieve the addresses of all other recipients in those fields. If you are sending an email to a list of people outside , where privacy of individuals might be relevant, place your list of recipients in the "Bcc" field and set the "To" field to your own address. This ensures that none of the recipients can retrieve the identities of the other recipients.

- Keep your operating systems up to date to prevent susceptibility to viruses.
- Scan email attachments to detect viruses and other malware.

Be aware that the monitors the use of electronic communications and web-browsing. Your manager can request reports detailing your activity if they suspect inappropriate use of email or web-browsing facilities.

Ask if you want further information.

Monitoring

The monitors all email for security purposes.

Specifically, communications may be monitored without notice and on a continual basis for a number of reasons including compliance with legal obligations, effective maintenance of IT systems, preventing or detecting unauthorised use or criminal activities (including cyber-intrusion), monitoring of service or performance standards, providing evidence of business transactions, and checking adherence to policies, procedures, and contracts.

In general, the monitors telephone usage, network, email and Internet traffic data (including sender, receiver, subject, attachments to an email, numbers called, duration of calls, domain names of websites visited, duration of visits, and files uploaded or downloaded from the Internet) at a network level.

Email threats

Although email is a powerful business tool, it has problems. In this guidance, we describe some of the problems, and how you can avoid them.

Email threats often use familiar email addresses to disguise attacks, or to pose as valid emails. Email threats are becoming more frequent and pose one of the biggest problems for systems and services.

There are many possible threats, including:

- Viruses: These can be spread between computers in emails or their attachments. They can make PCs, software or documents unusable.
- Spam: This is unsolicited mail sent in bulk. Clicking on links in spam email may send users to phishing websites or sites hosting malware. Often email spam mimics the addresses of people you know.
- Phishing: These are emails disguised to look like a legitimate company or bank to illegitimately obtain personal information. They usually ask you to verify your personal information or account details. Often links will direct you to a fake website, made to look like the real thing.
- Social engineering: In the context of security, social engineering refers to manipulating people to do something or divulge confidential information. For example, you might get a call from someone pretending to be from a software supplier, claiming that a virus has been found on your PC; they demand personal details before they can remove the virus.
- Spoofing: A spoofed email is where the sender (in this case, a criminal) purposely alters part of the email to make it look as though it was from someone else. Commonly, the sender's name/address and the body of the message are made to look as though it was from a legitimate source. It is commonly used to trick the recipient into providing confidential information such as passwords, or to market an online service dishonestly, or to sell a bogus product. Check the real sender of any email you receive if you ever have any doubt or uncertainty. If the sending address is one you don't recognise, do not click on any link contained within the email.

The scans approximately 14 million messages a month for threats (figures from November 2020). Of these, we might expect to find 1.4 million "spam" messages, 150,000 "phishing" messages, and about 1,000 malware messages (including viruses). Unfortunately, not every virus or spam email will be identified and blocked. The good news is that there are some simple steps you can take to reduce the threat:

- If you are not expecting the email, do not reply to it.
- If you are at all suspicious, do not divulge your details or any sensitive information.
- Avoid opening potential scam emails.
- Don't open unexpected attachments or click on strange links in emails, even if the email appears to be from someone you know. Check the style and content; if it isn't consistent with previous emails, it could be a scam.
- Do not reveal personal or other sensitive information in response to automatic email requests.

- Avoid sharing your business email address on the internet. These might be collected and used by automatic 'harvesting' software programs.
- Never use your email address to register for non-work related sites.

If you think you've received a scam email, or a virus, report it immediately. Do not click on any link or forward it to anyone. Only delete it from your inbox when you have been told to do so.

Further reading from the NCSC

Email security and anti-spoofing

Other email problems

Auto-forward

Auto-forwarding is where you get your email system to send emails automatically to another account. This might seem very useful, especially if for some reason you can't access your normal business email account, for example while you are away on holiday.

But auto-forwarding is very risky.

You can't be certain that the forwarded emails are safe to send to the new account. For example, the new account might have weaker technical security, making it easier for a hacker to break in and read your email.

You might also be auto-forwarding emails sent to you from outside the ; perhaps from another government department or commercial organisation.

When an email is sent to you, you are responsible for ensuring that everything in the email is handled correctly. This means looking after it to the standard required for that information. You mustn't send that information to another email address, where the required security standards might not be met.

Never use auto-forwarding to forward emails from your business email address to another non- email address. In particular, never forward email from your business email address to a personal email address.

There might be occasions when you have a genuine business need to auto-forward email to another email account, where the new address has the same or higher security standards. An example is forwarding from an business email address to another business email address. If you have business need for this, ask for help.

Chain letters

These are letters sent to several people who are asked to send copies to several others. They sometimes threaten that bad things will happen if the letter is not forwarded. Chain letters are a hoax.

Chain letters usually do not have the name and contact information of the original sender so it is impossible to check on their authenticity.

Legitimate warnings and solicitations will always have complete contact information from the person sending the message.

Newer chain letters may have a name and contact information but that person either does not exist or is not responsible for the hoax message.

Warnings without the name of the person sending the original notice, or warnings with names, addresses and phone numbers that do not actually exist, are probably hoaxes.

Don't circulate warnings yourself; real warnings about viruses and other network problems are issued for everyone by technical services.

Note: When in doubt, don't send it out.

Scams

Scams are "get rich quick" schemes. They make claims such as promising your bank account will soon be stuffed full of cash if follow the detailed instructions in the letter or email. In reality, it is an illegal plan for making money.

A typical scam includes the names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then remove that name and add yours to the bottom.

You are then supposed to mail copies of the letter or email to a few more individuals who will hopefully repeat the entire process. The letter promises that if they follow the same procedure, your name will gradually move to the top of the list and you'll receive money.

Other high-tech scams using IT also exist. They might be sent over the internet, or may require the copying and mailing of computer disks rather than paper. Regardless of the technology used to advance the scheme, the end result is still the same.

Scams are a bad investment. You certainly won't get rich. You will receive little or no money. The few pounds you may get will probably not be as much as you spend making and mailing copies of the letter if hard copy.

By their very nature, scams are harassing. Sending such mails using facilities is prohibited. The misuse of computer resources to harass other individuals or groups is unacceptable. Any person tempted to forward an email scam should familiarise themselves with the HR intranet pages, particularly the section regarding disciplinary action and electronic communications.

Note: Scams also clog up the system and reduce the efficiency of our servers.

How to recognise a scam

From the older printed letters, to the newer electronic kind, scams follow a similar pattern, with three recognisable parts:

- A hook: this to catch your interest and get you to read the rest of the letter. Hooks used to be "Make Money Fast" or "Get Rich" or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like "Danger!" and "Virus Alert" or "A Little Girl is dying". These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.
- A threat: when you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. Others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.
- A request: some older chain letters ask you to send money to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to "Distribute this letter to as many people as possible." They never mention clogging the internet or the fact that the message is a fake; they only want you to pass it on to others.

If it sounds too good to be true, then it is!

Bogus calls

There are a range of scams that can target you at home or at work. Callers usually say they are from IT Support, and tell you that they have detected a virus on your machine that needs to be removed. The bogus caller will then either:

- Direct you to a website, in the hope you will download malicious software.
- Try and obtain details from you about your computer, or the network.

In all genuine situations, the will provide you with an incident reference number if there is a real problem with your machine.

If you receive a call from someone claiming to be from the , always ensure you ask them for the incident reference number. Then disconnect the call, and call the yourself, directly. If the original call was genuine, when you provide the incident reference number, they will be able to help you.

In general:

- Treat all unsolicited calls as suspicious.
- If possible, note the details and incoming telephone number of the caller.
- Do not go to any external site if directed from an unsolicited call.
- Never give any information about your computer to the caller.
- Check if the call is genuine with your . Report the call as a security incident if it is not. Use a different phone from that used to take the original call.

Hoaxes

Hoax letters are designed to trick you into believing, or accepting as genuine, something false and often preposterous: the messages they contain are usually untrue.

Hoax messages try to get you to pass them on to everyone you know using several different methods of social engineering. Most of the hoax messages play on your need to help other people. Who wouldn't want to warn there friends about some terrible virus that is destroying people's systems? Or help this poor little girl who is about to die from cancer?.

Chain letters and hoax messages have the same purpose but use a slightly different method of coercing you into passing them on. Chain letters, like their printed ancestors, generally offer luck or money if you send them on (scams). They play on your fear of bad luck and the knowledge that it is easy for you to send them on. Scams play on people's greed and are illegal no matter what they say in the letter.

The risk and cost of hoaxes

The cost and risk associated with hoaxes may not seem to be that high. If, however, you consider the cost of everyone within the receiving one hoax message, spending two minutes reading it and another two minutes forwarding it on or discarding it, the cost can be significant.

Handling these messages may also make our mail servers slow down to a crawl or crash.

Spammers (bulk mailers of unsolicited mail) may harvest email addresses from hoaxes and chain letters. Many of these letters contain hundreds of legitimate addresses, which is what the spammers want. There are also rumours that spammers are deliberately starting hoaxes and chain letters to gather email addresses.

How to recognise a hoax

A request to "send this to everyone you know" (or some variant) should raise a red flag. The warning is probably a hoax. It's unlikely a real warning message from a credible source will tell you to send it to everyone you know.

If the warning uses technical language, most people, including technologically savvy individuals, tend to believe the warning is real.

There may be credibility by association. If the janitor at a large technological organisation sends a warning to someone outside of that organisation, people on the outside tend to believe the warning because the company should know about those things. Even though the person sending the warning may not have a clue what he is talking about, the prestige of the company backs the warning, making it appear real.

These make it very difficult to be certain a warning is a hoax. Check if the claims are real, and if the person sending out the warning is a real person. Ask yourself if they are someone who would know what they are talking about.

Type of hoaxes

Scam chains

Mail messages that appear to be from a legitimate company but that are scams and cons, for example Advance fee scams.

Giveaways

Stories about giveaways by large companies. If you only send this on, some big company will send you a lot of money, clothes, a free vacation, etc., etc. You would have to wait forever for any of these to pay off.

Malicious warnings (virus hoaxes)

These are warnings about Trojans, viruses, and other malicious code, that have no basis in fact.

Virus hoaxes have flooded the internet with thousands of viruses worldwide. Paranoia in the internet community fuels such hoaxes. An example of this is the "Good Times" virus hoax, which started in 1994 and is still circulating the internet today. Instead of spreading from one computer to another by itself, Good Times relies on people to pass it along.

Sympathy letters and requests to help someone

Requests for help or sympathy for someone who has had a problem or accident.

Urban myths

Warnings and stories about bad things happening to people and animals that never really happened.

Inconsequential warnings

Out of date warnings and warnings about real things that are not really much of a problem.

True legends

Real stories and messages that are not hoaxes but are still making the rounds of the internet.

Traditional chain letters

Traditional chain letters that threaten bad luck if you don't send them on or request that you send money to the top "x" people on the list before sending it on.

Threat chains

Mail that threatens to hurt you, your computer, or someone else if you do not pass on the message.

Scare chains

Mail messages that warn you about terrible things that happen to people (especially women).

Jokes

Warning messages that it's hard to imagine anyone would believe.

Email and storing information

Data held by the should be managed in such a way that employees who require the data, for business reasons, can gain access to it. Managers should ensure that data is stored in an area that is easily accessible to those who require access. This includes information exchanged using email.

If you need further assistance or information about this process, ask for help.

Accessing emails or information in an absent employee's email account

Staff absences do occur and these can cause disruption to business where colleagues have no access to relevant departmental information. Staff are away for events such as annual leave, secondment or maternity leave, but they don't make provision for colleagues to access departmental information.

When an absence occurs, there is no right to be able to access another employee's account to obtain information. This is true, regardless of whether the absence is expected or unexpected, for example annual leave or illness.

Accessing another employee's account, without their permission, might contravene data protection legislation.

Data protection legislation protects personal information which relates to identifiable, living individuals held on computers. It specifies that appropriate security measures must be in place to protect against unauthorised access to, loss or destruction of personal data. If you breach this principle you could render the liable to enforcement action by the Information Commissioner.

Avoiding the problem

If you know you're going to be away for any significant amount of time, you can make life easier for everyone, including yourself, by following these simple steps:

1. Make provision for someone to have access to your work email account during your absence. If you don't know how to do this, contact your .
2. Create a "handover" package, containing information about the tasks that will, or might, need attention during your absence.
3. Make sure the package has contact details for everyone who might need to help progress or update the status of the tasks.
4. Create an "Out Of Office" notification in your email system; include clear details of who to contact in your absence.

Authorised access to user email accounts

You must not access the email accounts of any other users, unless you are authorised to do so as required by your role. Access is authorised on a case by case basis only, and will typically be aligned to the following circumstances:

- During a criminal investigation by a law enforcement agency.

- During an employee investigation relating to misconduct or a security incident, for example IT misuse.
- Upon the death or unexpected exit of an employee, for example for the retrieval of key information and closing down an account.

Ideally, access will have been organised in advance of an absence. But this is not always the case; sometimes there are unexpected or unusual circumstances. Gaining access in such situations will require substantial escalation to management and Data Privacy and Security teams.

Contacts for getting help

In practice, all sorts of things can go wrong with email from time-to-time. Don't be afraid to report a problem or ask for help; you'll be creating a better and safer work environment.

For general assistance on security matters, email .

Suppliers to the should primarily contact your usual points of contact.

General app guidance

When working, you need to communicate with colleagues and use business tools ('apps'). You'll also need to work with people outside the . There are various tools you might use, besides the standard email and telephone tools. This document tells you about the tools you can, and cannot, use for business purposes. This guidance applies to all staff and contractors who work for the .

Some ALBs, Agencies, or other large groups within the might have their own, specific guidance regarding how to use certain apps for different purposes.

Access to tools

You can access tools that are provided through your provided devices by downloading from:

- The Software Centre application on your device (for Dom1 equipment).
- The Self Service application on your Mac (for managed MacBook laptops).

Currently, access to the tools mentioned in this document is not available from Quantum devices.

For other provided devices, seek help from your Line Manager in the first instance.

Corporate, work and personal accounts

- A corporate account is for making official statements and providing official views. Only a small number of authorised people can use it.
- A work account is your normal account, that you use every day for business as usual. Only you have access to your work account.
- A personal account is your own personal account on gmail, hotmail, yahoo, and so on. You should never use a personal account for business purposes. To be clear: never send your work material to your personal device or your personal email account.

Some of the applications listed make a distinction between general use with a work account, and use with a corporate account. Using a tool with a corporate account means you are providing views or statements on behalf of the . Never use a personal account for business purposes with any tool.

Remember that if you are authorised to use a corporate account, you are speaking and acting for the whole of the . When working with a personal account, you are speaking and acting as an employee and a civil servant.

Always follow all policies and guidelines regarding public information, including social media. To access this information you'll need to be connected to the Intranet.

In particular, follow the Civil Service Code of Conduct.

Video conference hardware

There are specific security concerns when using video conferencing hardware. The hardware might need extra permissions, involving access to the network, or involving personally identifiable information.

Video conferencing hardware might also be in a 'constant listening state'. This means that anything said within hearing distance, at any time, is 'heard' by the device. Similarly, anything in the line of sight might be 'seen' by the device. Some video conferencing hardware might record and even store the audio or video data outside the .

Video conferencing hardware for use within the meet the required security standards of the . Any devices that do not meet the security standards be used. The reason is that the hardware might be insecure, and therefore unsafe to use for conversations.

Using video conference tools safely

The NCSC has excellent guidance on using video conferencing services safely.

Key things to remember *before* a call include:

- Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password.
- Test the service before making (or joining) your first call.
- Understand what features are available, for example recording the call or sharing files or screen information.

Key things to remember for *every* call include:

- Do not make the calls public, for example always require a password to join the call.
- Know who is joining the call, in particular check that everyone is known and expected to be present, and that people who have dialled in have identified themselves clearly and sufficiently.
- Consider your surroundings, for example checking what can be seen behind you (forgetting to check information on a whiteboard or noticeboard is an easy mistake).

Policy and guidance
and Information

information is the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

is not a classification. is a handling caveat for a small subset of information marked that requires special handling by staff. You should apply the handling caveat where you wish to control access to that information, whether in a document, email, or other form.

Privacy and personal information (Data Protection)

Some communications tools expect to have a copy of your contacts list. The list is uploaded to the tool server in order to let the tool to function correctly. Think carefully about whether this is reasonable to do. Make sure that sharing your contacts list does not impact any one else's privacy in a negative way.

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice:

- Email:
- Slack: `#security_privacy_and_live_service_team`
- Intranet: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/

Information Management

Many of the tools are only used for your day-to-day communication with colleagues. The information you work with is typically classified at .

Think about the information you work with when using these tools. What would happen if you lost your mobile device, or it's stolen? Suppose the voice or video call was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is 'No', then it's probably OK to use the tool to communicate that information with colleagues.

You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is Principle 2 of the Government Security Classifications. The trusts you to work with information. You're trusted to make a reasoned judgement about whether it's safe to use an approved tool, or whether you should use a different -provided work tool.

Never send work material to your personal devices or email accounts.

Remember that it is impossible to delete information after it's released in public.

For more information about IT Security, look on the Intranet here.

Storage and data retention

Laws and regulations make the and its employees responsible for managing information. Some examples include:

- Freedom of Information Act.
- Data Protection Act and General Data Protection Regulation.
- Public Records Acts.

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate systems helps us, because:

- We can provide evidence about decisions.
- We understand the information held, and where to find it.
- We can transfer records to The National Archives.

Always store information in systems. If you use a tool for work tasks, make sure the key information is stored in an appropriate system. Guidance on what you must keep is available on the Intranet here. At regular and convenient intervals, transfer the information to an appropriate system. Do the same when you finish the work. Don't forget to remove any redundant information from a tool by clearing or deleting data if it has been preserved in an system.

Many tools lets you export your data. You can then store it on an appropriate system. Sometimes it's easier to copy and paste text into a new document. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

For more guidance, read the Information Management section on the Intranet. There is also help on responding to requests for information.

Acceptable Use

You must use communications tools for business purposes in an acceptable way.

Be sensible when using communications tools for business purposes:

- Be extra careful with sensitive and personal information in tools.
- Try to avoid using the same tool for business and personal use - you can get confused who you're talking with.
- If the message you're about to send might cause problems, upset, offence, or embarrassment, it's not acceptable.
- Context is important - a message you might think is funny could be upsetting to someone else.
- If something goes wrong, report it.

The bottom line is:

> If there is doubt, there is no doubt - ask for help!

Approved tools

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Apple Facetime	Communication tool: Video	Avoid personal or sensitive data	Smartphone App	Internal/ External
Apple iMessage	Text messaging	Avoid personal or sensitive data	Smartphone App	Internal/ External

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Google Meet (was Google Hangouts)	Communication tool: Video and/or voice	use approved for and	controlled Mac - Self service, Web browser.	Internal/ External
Microsoft Teams	Communication and collaboration tool: Video and/or voice	use approved for and	Dom1 Software centre, controlled Mac - Self service, Web browser.	Internal/ External
Miro	Collaboration tool: Whiteboarding	Avoid personal or sensitive data	Web browser.	Internal/ External
Skype for Business	Communication tool: Video and/or voice	use approved for and	Dom1 Software centre, controlled Mac - Self service, Web browser.	Internal/ External
Slack	Text messaging, Voice/ Video calls, etc.	Avoid personal or sensitive data	controlled Mac - Self service, Web browser.	Internal/ External
Slido	Q&A tool during presentations	Avoid personal or sensitive data	Web browser.	Internal
Trello	Project management tool, 'Kanban' cards	Avoid personal or sensitive data. An enterprise-wide licence is available. Ensure you create Trello boards in the workspace. Do not use a personal Trello account.	Web browser based use. Log in using your single sign-on account, for example a Digital & Technology Google account, or a Microsoft Office 365 account.	Internal
Twitter	Text Messaging, Video transmission	Approved for Corporate account. Using a personal account to comment on work related issues is encouraged, as long as you follow the Civil Service Code of Conduct.	Web browser, Windows 10 App, Smartphone App.	Internal/ External
WhatsApp	Text messaging, Voice/ Video calls	Avoid personal or sensitive data	Dedicated app on device, also web browser.	Internal/ External
Yammer	Text messaging	Avoid personal or sensitive data	Dedicated app on device	Internal
YouTube	Video sharing tool: Video, streaming and chat	Avoid personal or sensitive data	Web browser based use.	Internal/ External
Zoom	Communication tool: Video, voice and chat	Avoid personal or sensitive data	Web browser based use, or dedicated and installed app by approval	External meetings. For Internal meetings, use Microsoft Teams.

Password managers

guidance encourages the use of password managers where possible. To establish what options are available for an -issued device, check the official software and application installation tool provided with the device, to see whether it includes a facility to install optional software and whether a password manager is among the options.

Tools for sharing information internally and externally

For secure sharing and transfer of materials within bodies or external organisations including other government departments, the installation of Microsoft Teams is approved for use with data up to and including .

For secure sharing and transfer of materials with external organisations that cannot use Teams, the Criminal Justice Secure Exchange (CJSE) and Criminal Justice Secure Messaging (CJSM) tools are the preferred solution for data up to and including .

For secure sharing and transfer of materials with external organisations where the use of Teams, CJSE, or CJSM is not practicable, the following tools are approved for data up to and including :

- Egress (NCSC certified)
- Galaxkey (NCSC certified)

For use within bodies, these products may only be installed on -issued devices. For advice on installation and configuration of these products, consult the team responsible for the supply and configuration of your devices.

For secure sharing and transfer of materials with other government bodies, where the use of Teams, CJSE, CJSM, Egress, or Galaxkey is not possible, the use of official email systems is approved for data up to and including .

Always follow the guidance in the Data Handling and Information Sharing Guide when making such transfers. This applies particularly with regard to the sharing of data classified higher than .

If you need clarification or further assistance in selecting the appropriate tool, ask for help.

Proctoring software

You install proctoring software onto equipment.

Some certification or examination organisations enable people to take assessments remotely. They do this by having 'supervision' software installed on the user's computer. This software is often referred to as 'proctoring software'. The tools make sure that the assessment is as fair as possible, by installing a variety of controls. For example, the software can take control of the camera and microphone of the device it is installed on.

The problem is that the controls give the proctoring software extensive access to the computer. This means that the tools could inspect information or other applications on the computer. In effect, the proctoring software might have uncontrolled access to information or materials on the computer. This is not acceptable.

If you need to use proctoring software, your options are:

- Install the proctoring software on a personal device.
- Contact the assessment organisation asking for alternative options.

NHS Track and Trace

The official NHS Covid-19 app was designed by the NHS. Both NCSC and Cabinet Office have been involved in the security of the system. The app provides contact tracing, local area alerts and venue check-in. It enables you to protect yourself and your loved ones. Installation is optional, but recommended.

After installing the app, you'll receive an alert if you have been in close contact with other people who have tested positive for coronavirus. You can then take action to avoid passing the virus on, for example by self-isolating.

From a security perspective, it is safe for you to use the app on your personal or issued devices. There are no extra risks for colleagues with security clearance, such as SC and DV.

If you wish to install the app, start at the NHS site.

Note: The NHS app may not work on some older devices. Installation might not be possible, for example on Quantum smartphones.

You might have both a personal and an issued device. Think about which device makes most sense to use with the app. It's best to install on the device that you carry with you and use most of the time. You could install on all your devices if you prefer.

To reduce the likelihood of false alerts on the app, turn off the app's Bluetooth mode. Do this when:

- You are working in environments with protective Covid measures in-place, for example plexiglass separators.
- You need to leave your personal or work device in a locker, for example during a sports activity or to work in a secure facility.

Other tools

Some tools, such as Facebook, Instagram and LinkedIn, are approved for specific corporate accounts to use, for corporate communications messages. General use of these tools for work purposes is not permitted.

If you wish to use a tool that is not listed in this guidance, please consult our Guidance for using Open Internet Tools and ask for help.

Other information

Government policy and guidance

GDS Social Media Playbook

NCSC

Video conferencing services: using them securely

Secure communications principles

Using third-party applications

Phishing Guide

This guide provides information about 'phishing' is. It describes what phishing is, and how it happens. It tells you what you can do to protect yourself, and to keep systems secure.

There is also information on what to do if you think you have been phished.

What is a phish?

Phishing attacks are when threat actors pretend to be legitimate parties. They do this to steal money, credentials, or sensitive information. There are a variety of phishing attacks that you might come across. Some are more sophisticated or targeted than others.

Phishes often use two techniques:

- They affect emotional states.
- They create a sense of urgency.

Urgency makes users want to do the actions requested as quickly as possible. The combination of urgency and emotional manipulation leaves users feeling panicked and worried. It might fill them with a sense of euphoria. Threat actors use emotion and deadlines to convince users to act. The user doesn't take the time to think about whether it's a sensible or valid request.

Most phishes are emails, but they can also use other technology, such as SMS texts or telephone calls.

Threat actors might use phishes to request payments. They might ask you to click links and log in to an account or change a password. They might instruct you to buy items for them. They might get you to provide some personal details before you can claim a supposed prize.

Threat actors utilise a variety of methods in phishes. They often take advantage of seasonal events to appear more legitimate. They use emotional and urgent triggers such as:

- Telling you that your tax return is overdue.
- Threatening to share access to your personal sensitive photos unless you pay.
- A request to send money urgently to a family member in trouble.
- Telling you 'good news' ,for example that you have won a big prize or are due a tax rebate.
- Providing a final demand about a very overdue invoice that, if unpaid, will see you taken to court.
- A 'last warning' about resetting your password, otherwise you will lose account access.

Beware of messages that create a sense of urgency or a heightened emotional state - good or bad. Treat such messages with suspicion. Check the message before you take any action. Unexpected messages with attachments are also common. Never open the attachment until you have done checked and verified the legitmacy.

Common types of phish

There are many different types of phish. You might recognise many of them. But the more sophisticated the phishing attack, the harder it is to spot. Checking and verifying are the best way to stop a phishing attack. They use a second, different method of communication to check the authenticity of the contact and the requested action.

Email phishing

These are emails that request actions. Examples include clicking on links to change passwords, or requesting money.

SMS phishing (smishing)

These are text messages that ask you to click links to access services or to pay for things. They often take advantage of seasonal events to appear more legitimate. Examples include Christmas delivery phishing texts, or texts around tax return time. Other recent examples use Covid news items to demand payments or personal information.

Voice phishing (vishing)

These are phone calls that ask you for sensitive information, or payments, or remote access to your devices. Threat actors might pretend to be from banks and other official organisations. Others might claim to be technology companies such as Microsoft. Another vishing example might claim to be from a jail, requesting bail money.

Spear phishing

Some phishing attacks focus on specific targets. Threat actors use OSINT to gather data about an individual. They can then create a 'custom phish'. It is interesting for the target. The target is then more likely to respond to the phish. Examples include real names or work-related jargon. These are often very sophisticated phishes. The use of personal data makes the phish more likely to succeed.

Whale phishing (whaling)

These target at high level individuals such as CEOs and Director level and above staff. Whaling uses a variety of phishing methods to contact high profile targets. The goal is to steal large sums of money, or access high level credentials, intellectual property, and sensitive information.

Business email compromise (BEC)

This type of phishing attack targets high level staff to steal money or reveal sensitive information. Threat actors pretend to be another high-level staff member. They do this by using their name or email address to seem legitimate. They often create a sense of urgency to convince junior staff to do the requested action. These emails often come from a compromised staff member's email account. This means the email system doesn't block the sender.

Watering hole attack

This is a very sophisticated supply chain attack. It uses research from an organisation's frequently used websites to identify a target. Targeted websites are then compromised and infected with malware. When users visit the websites, the malware downloads onto their systems. These are sophisticated attacks. The user is visiting an official and legitimate website. It is the website itself that has been compromised.

QR codes

Quick response codes (QR Codes) are a form of matrix (two-dimensional) barcode. They are machine-readable links. A QR code reader on a mobile device sends the user to a website or app. You don't need to click or type a link.

Some devices have QR code readers built into their camera app. Other devices need a dedicated app.

When you scan the QR code, the app asks you if you wish to go to the website or app described by the QR code.

Note: QR codes are not human readable. This means it is important to verify that the codes are legitimate and have not been tampered with.

You'll see QR codes in many situations. They give easy access to restaurant menus. They link to charity donation pages or surveys. Banks use them to link to services. They can be used to join wifi hotspots. They can be used to add contacts directly to your contacts list.

A QR code in an official context should be as safe to scan as an ordinary web link. For example, a QR code on an official notice in an building.

If the QR code is not labelled, or is from an unknown person, be suspicious. For example, a QR code stuck on a lamppost, or a QR code on a non-official flyer on a wall in a public location. These are not safe to scan.

It's possible that even a QR code in a safe, official place might be tampered with. Someone might draw over it. They might cover it with a sticker and a fresh QR code. If a QR code looks 'contaminated', don't scan it. Report it to security.

In summary, the risk associated with QR codes is currently considered low. They are simply barcode versions of web links. When deciding whether to scan a QR code or not, follow the same procedure as receiving an unexpected message .

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is a great way to reduce the risk of account compromise by a phishing attack. MFA provides an extra layer of defence for the account. If you have MFA set up, threat actors cannot access your account. It's safe, even if you accidentally reveal your credentials.

Never give MFA to codes to anyone. Genuine companies, banks, government departments, and social media sites will never contact you and ask you to tell them an MFA code. They will never offer to input it for you, or request you give the code to them over the phone. MFA codes should only ever be entered by you, directly into the account login.

MFA also provides an early warning system for credential compromise. If you ever receive an MFA code for an account that you are not actively logging into, then someone other than you is trying to access the account. This means your credentials might have been compromised, so as quickly as possible, you should:

- Report the problem to security.
- Change your password.

Check and Verify

Check and verify is an easy method to confirm the legitimacy of communications and requests. They can confirm the identity behind a message or request, and they can confirm the validity of the message or request itself. Social engineering techniques and phishing tactics take advantage of people who do not use check and verify. By checking and verifying, these sorts of attacks can be stopped very easily.

Checking and verifying is when an individual uses a different method of communication than the one the message came from. This method means that if one communication method is compromised, you quickly find out by using a different communication method to confirm validity. The likelihood of multiple communication methods for the same person or team being compromised is low.

Example 1: You receive an email request for an urgent review of an invoice, and immediate payment. The email comes from someone unexpected. You should find the official contact details of that person, and contact them using a phone call – but not email – to confirm that they did indeed send the original email. If they did send the email, you can proceed with the request. If they did not send the email, you can report the email as a phish, and also alert the owner of the email address that their email address might have been compromised.

Example 2: You receive a phone call from someone claiming to be your bank, or HMRC, or HMCTS. You hang up the call, and locate the official website for the company. You should be able to find multiple official contact details there. Use one of these to contact the place the caller claimed to be from. If, for example, the claim was that your bank was calling, you can call the direct number and speak to the switchboard about the reason for the initial call. They will forward you to the correct department. You can then confirm the validity of the original call, and so confirm whether the original caller was actually from your bank or not.

Example 3: Someone enters your place of work, and claims to have a meeting with a specific person. Unfortunately, there is no record of this on the expected visitor list. You can call or email the person within your place of work to confirm the visitor is legitimate. This check also works if tradespeople arrive unexpectedly, because you can contact both the relevant person within your place of work and also contact the company they claim to be from, using the company's official website contact details.

Example 4: You receive an email requesting that you reset your password immediately. The email contains a link to perform the password reset. You have not attempted to login to that account recently. You should use an internet search for the website or type the URL directly if you know exactly what it should be. When you attempt to login, the website will let you know if you need to reset your password. If not, you know someone else has attempted to gain access to your account. That would mean the password reset request was not legitimate, and most likely a phishing attempt hoping to get your username and password through the reset link in the original email. Similarly, if you get an MFA request unexpectedly, do not confirm it unless you were indeed attempting to access that account immediately before the request came through. If you get an MFA request, but had not been trying to connect using the account, you should change the account password as soon as possible, because it might have been compromised.

When checking and verifying, be sure to pick a different method of communication to the one used to contact you originally. If someone emails you unexpectedly, check and verify by making a phone call. If someone calls you, check and verify by using the Internet. It is very unlikely that multiple communication channels have been compromised.

Be sure to get official contact details for companies only from their official websites. Never be afraid to hang up on someone and check their identity through another method, especially if they are asking for sensitive or personal information or credentials. Never be afraid to check the legitimacy of unusual email requests. by contacting the sender through a different communication channel.

By checking and verifying, it lets you confirm that the messages come from the person they claim to be, and that the requests are valid. This helps prevent you or your company from losing money to fake invoices, from accidentally giving up sensitive information or credentials, and from having unauthorised individuals in your place of work. Checking and verifying is fast and easy. All members of your workplace should be happy to receive such a check. It shows that you take security seriously, and that you are helping to protect them as well as yourself.

If you think you've been phished

Don't panic.

You will not be punished if you fall for a phish - it can happen to anyone. You will not be punished for reporting a phish, even if it turns out to be a false alarm.

If you think you have been phished:

1. Report it immediately.
2. If your credentials were phished, highlight that in the report.
3. Change the password for affected accounts as soon as possible. Never use the link in an email asking you to change a password. Check and verify by going directly to the website to change a password. Be cautious when following password actions requested in emails or texts.

firewalls and antivirus systems should catch the majority of malware before they can affect systems. By reporting the incident as quickly as possible, the security team will be alerted and on the lookout for any more sophisticated malware.

If your credentials have been phished, reporting it immediately and resetting your password quickly greatly reduces the risks.

Any phishing emails that get through the filters and into your inbox will be very sophisticated. This makes them much harder for you or anyone to spot. Never feel guilty or ashamed for being phished.

Reporting phishes

Reporting phishing attempts helps improve the filters that catch them before they get to your inbox. They also help protect other colleagues and the from being compromised, or having data or money stolen.

If you think you have spotted a phish, or you think you have been phished, report it as quickly as possible. If you think you have spotted a more targeted phish that claims to be from a vendor or another staff member, check and verify to determine if it is legitimate. If it is not, then please report the email as a phish.

Reporting a phishing attempt is quick and easy. Contact service desk using one of these two options:

You can also forward on all spam and phishing text messages to 7726 for free.

Protecting WhatsApp accounts

The permits the use of WhatsApp for text messaging, voice and video calls. You avoid using it for business tasks involving personal or sensitive data.

You always keep WhatsApp account details safe and secure. Accounts link with specific devices. When you register your device with a WhatsApp account, that provides some protection. Only the registered device can send or receive messages associated with you.

Unfortunately, device registration is a tempting target for attackers. It is a way for potential compromise of user data. Compromises affect backups of conversations, and contact lists.

A compromised account might also attack other people. An attacker might pretend to be a user, and so target other contacts. They might make their way to compromise a high-value target.

An example scenario might be an attack on the WhatsApp account of a family member of an employee. The attacker compromises the family member's WhatsApp account. They then pretend to be the family member. They contact the employee through the contact list. The employee trusts the message: it seems to come from the family member.

How a WhatsApp attack works

Note: This document does not provide full details of how to attack a WhatsApp account. We provide enough information to understand helpful protective steps.

Registering a device with a WhatsApp account uses an authentication code (a PIN code). The attacker tricks the victim into revealing the device registration code. They then deregister the victim's device from the WhatsApp account. Next, they register the attacker's device with the WhatsApp account.

The key point is the authentication code. It's very important to keep this secret, like a password.

Recovering and protecting your WhatsApp account

You can often recover a compromised WhatsApp account. A good way is to use your device telephone number. Use the app to ask for a 6-digit SMS verification code. When the code gets to your phone, enter it into the app. After re-authenticating your phone, the attacker is automatically disconnected. They cannot reconnect without a fresh authentication code.

While recovering an account, you might have to provide a two-step verification PIN. If you don't have this code, it suggests the attacker enabled two-step verification. Without the code, you must wait 7 days before you can sign in to WhatsApp. But the attacker is disconnected from the account immediately when the code is sent. Although you can't get into your account for a week, the attacker cannot get into your account at all.

When you reconnect into your WhatsApp account, check for any unknown devices. Do this by checking **Linked Devices** in the WhatsApp settings menu.

Always enable two-step verification on your account. Any future attempt to register a device needs a PIN to enable the app. Do this by going into the **Settings** then **Account** menu on the app. Select the **Two-step verification option**.

If there's something suspicious about your account, or the messages in the account, contact the . Ask for help as soon as possible.

Always follow policy about applications for official business or storing business-related information. Don't use unapproved applications for official business. Don't use unapproved applications for storing business-related data. Always use approved applications and storage tools.

WhatsApp account do's and dont's

Do ask for help if you think your WhatsApp account has been compromised.

Do enable two-step verification on your account. Do this by going into the **Settings** then **Account** menu on the app. Select the **Two-step verification option**.

Do tell everyone on your contact list if you think your WhatsApp account has been compromised.

Do check the list of linked devices at regular intervals. Look for unknown or unexpected devices. Do this by checking **Linked Devices** in the WhatsApp settings menu.

Do not share a WhatsApp one time passcode, password, or authentication code with anyone.

Do not use unapproved or unauthorised applications for work purposes.

Do not use personal accounts for work purposes.

Secure Data Transfer Guide

Introduction

This guide outlines the security procedures and advice for staff wanting to send or receive data securely from external sources.

This is important to the , because personal and sensitive data is regularly transmitted between departments. Legislation such as GDPR, and industry standards such as PCI DSS, affect the 's responsibility to secure this data. It is also important to recognise the damage that leaked sensitive data could cause to the vulnerable people the works to protect.

Who is this for?

This policy is aimed at three audiences:

1. **Technical users**: these are in-house Digital and Technology staff who are responsible for implementing controls during technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
2. **Service Providers**: defined as any other business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, storing data) for, or on behalf of, the .
3. **General users**: all other staff working for the .

The phrase "all users" refers to General users, Technical users, and Service Providers as defined previously.

Transfer Considerations

Anyone handling personal or sensitive data must seek consent from their line manager to authorise data transfer.

Before any data transfers are requested, consider the following:

- Is it strictly necessary for the effective running of the , and the care of the people it serves, that the data (regardless of whether the data is sensitive or not) is transferred?
- What is the nature of the information, its sensitivity, confidentiality, or possible value?
- What is the size of the data being transferred?
- What damage or distress might be caused to individuals as a result of any loss or unmanaged sharing during transfer?
- What implications would any loss or unmanaged sharing have for the ?
- What information is actually necessary for the identified purpose? For example, is the intention to send an entire document or spreadsheet, when only one section, or specific spreadsheet columns, are required?
- Has the identity and authorisation of the information recipient been established?

Any transfer technique used :

- Encrypt the data over the network (in transit), using sufficient and appropriate encryption (currently TLS 1.2 or greater).
- Require strong authentication to ensure that both the sender and recipient are who they claim to be.

These considerations apply when transmitting any data over a wireless communication network (for example wifi), or when the data will or might pass through an untrusted network.

If the is the controller of the data being transferred, the security storage requirements at the destination be considered to ensure that they comply fully with the relevant regulation, such as PCI DSS or GDPR.

If it's not clear who the data controller is, ask the for help.

When dealing with third parties, consider whether any data sharing agreements or contracts are in place that apply to the transfer of that data. Check whether there are any stipulations in place regarding the method of transfer that can or should be used.

If personal data is being transferred to a third party, then the privacy team be informed, to decide if a Data Protection Impact Assessment is required.

Data Transfer

Normally, files be transferred by email. Normally, files be transferred by secure network links using appropriate protocols such as `https`, `ssh`, or `sftp`. For large files, such as those over 5MB, transfer using a secure protocol is a practical necessity, as many recipients will not accept emails with attachments greater than 5MB.

Data Transfer by Secure link

The 's preferred method of data sharing is to use Microsoft Teams via Sharepoint. Teams has been authorised to hold information. It is configured to provide greater granular protection through tools such as Azure Information Protection (AIP). Where possible, data be transferred using Teams.

Due to the diverse nature of the 's architecture, using Teams might not always be possible. Those in the Digital and Technology team who do not have access to Microsoft Teams use to transfer data.

For more details on the actual process for a transfer, contact the .

Data Transfer by email

Where it is not possible to use Microsoft Teams or , **AND** the data to be transferred is less than 20MB, email be used, **BUT** the following requirements be met:

- Email communication be used to transfer unencrypted sensitive or personal data. Employees note that emails are not designed to attach and transfer large amounts of data. The 's email system does not support file attachments that exceed a total of 20MB.
- You consider an alternative secure method of transferring sensitive data wherever possible and practicable. If no suitable alternative is available, then apply an extra level of security. Do this by using encryption to apply a strong password to the sensitive data you wish to send. All passwords be transferred using an alternative method of communication to get to the recipient. Examples includes post, a telephone call to an agreed number, or by SMS text message.
- Email messages contain clear instructions of the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.
- Information sent , where practical, be enclosed in an encrypted attachment.
- Care be taken as to what information is placed in the subject line of the email, or in the accompanying message. Filenames or subject lines reveal the contents of attachments. Filenames or subject lines disclose any sensitive personal data.
- Emails only be sent from your work email address, as provided by the . This is to ensure that the correct privacy and security information is displayed.

CJSM email

- The Criminal Justice Secure email Service (CJSM) is provided for criminal justice agencies and practitioners to communicate with each other.
- As a general rule, it only be used for purposes relating to the criminal justice service.

Microsoft 365 Encrypted email

- This facility is available for standard individual and generic email accounts
- This method be used to send or receive files classified as . It is normally used with external partners, agencies, or individuals who cannot be contacted using CJSM email.
- The attached files on a single email exceed 25MB.

Removable storage devices

The strongly discourages the use of removable storage devices such as USB devices for data transfer. However, if all other options are not possible, then removable storage devices be used with caution.

Any data being transferred by removable media such as a USB memory stick be encrypted. Encrypted portable storage devices be password protected with a strong password. All passwords be transferred using an alternative method of communication to get to the recipient. Examples includes post, a telephone call to an agreed number, or by SMS text message.

If you think you have no other option for copying or moving data, and have to use removable media, contact the .

Ownership of any removable media used be established. The removable media be returned to the owner on completion of the transfer. The transferred data be securely erased from the storage device after transfer.

Clear instructions of the recipient's responsibilities, and instructions on what to do if they are not the intended recipient, accompany the removable media.

Any accompanying message or filename reveal the contents of the encrypted file. The sender check, at an appropriate time, that the transfer has been successful, and obtain a receipt. An email confirming receipt is acceptable.

Report any issues to your line manager and in the case of missing or corrupt data to the immediately.

Data transfers by post or courier

Data transfers using physical media such as memory cards or USB devices only be sent using secure post. Royal Mail First or Second class be used. Royal Mail Special Delivery or Recorded Delivery be used. For non-Royal Mail services, a secure courier service be used, with a signature obtained upon delivery. The recipient be clearly stated on the parcel. The physical media be securely packaged so that it is not damaged in transit.

The recipient be told in advance that the data is being sent, so that they know when to expect the data. The recipient confirm safe receipt as soon as the data arrives. The sender responsible for sending the data is also responsible for confirming the data has arrived safely.

Hand Delivery and Collection

Hand delivery or collection of data be used where removable media is used. When arranging for an individual to collect information, the identity of the individual be established, to confirm who they claim to be. An appropriate form of identification be provided before handing over any documentation.

Telephone or Mobile Phone

Phone calls might be monitored, overheard, or intercepted. This might happen deliberately or accidentally. Take care to protect calls, as follows:

- Transferred information be kept to a minimum.
- Personal or Confidential information be transferred over the telephone, unless the identity and authorisation of the receiver has been appropriately confirmed.

Residual risks with encrypted data transfer

All users recognise that even if a system uses encrypted data transfer, there are still occasions where data might be affected by unauthorised access. Be aware of these residual risks. Line Managers include consideration of these risks in employee awareness training. Examples include:

- Some data relating to the communication might still be exposed in an unencrypted form. An example is metadata.
- Data transfer processes that rely on Public Key Infrastructure (PKI) implement strict certificate checking to maintain trust in end-points.

Sending information securely

This guidance complements the overall security policy.

This guidance on working securely with paper documents and files applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, occupied premises.

Agencies and arm's length bodies (ALBs) are expected to comply with this corporate framework but may establish their own arrangements tailored to operational needs and should supplement it with local policy or guidance for any business-specific risk.

Related information

IT Security Policy (Overview) on page 16

Objective

The requires employees and contractors to get into the habit of looking after the information that they work with, whether it's on paper or stored electronically, in the same way they would take care of their personal valuables.

Scope and Definition

This guidance helps you understand the risks involved in sending information. It covers any information that relates to the business of the , its stakeholders and partners that have been printed out or written down on paper, and information that has been downloaded from IT systems onto 'removable media'.

This guidance outlines the all the basic guidance on sending information using email, post, courier services and fax.

Context

All information is valuable, and staff are expected to protect everything that relates to the department's business, including information provided by others. This applies to all information, not just information that is covered by the Data Protection Act or classified under the Government Classification Scheme.

There are different rules for managing and protecting different kinds of paper-based information. You need to know how to:

- Identify the correct security level for the information you work with.
- Handle it according to the relevant rules.

Responsibilities

All employees, contractors, partners, service providers and employees of other organisations who are on premises and co-located sites remain accountable for the security, health and safety of themselves, colleagues and the protection of departmental assets.

Policy statements

Using email

Email is the preferred option for securely transferring information between yourself and another civil servant. You use departmental equipment and transfer between or CJSM email accounts.

If the person or organisation you are sending the information to is outside departmental or CJSM networks, you consider the sensitivity of the information. It might be safer to send it on encrypted removable media or in hardcopy.

Sending bulk information

Transferring bulk data be authorised by a senior manager.

The definition of bulk or high volume is not specific. Removable media such as laptops, disks or memory sticks can hold thousands of records. They have the benefit of encryption to prevent access to data accessed, but the damage if they are lost and the information cannot be retrieved remains high. However, information is immediately accessible if even a single paper files is lost, so the risks need to be managed differently.

As an indication, datasets containing the electronic records of 1,000 or more people would count as bulk, whilst decisions on using more secure forms of movement might apply to much smaller volumes of case files. It might also apply to lesser volumes where names and addresses are combined with sensitive information that might lead to identification.

In all cases, consideration be given to the risk and impact of causing individuals or the to suffer harm or loss, service disruption, or reputational damage.

Using post and couriers

There are a range of methods of sending documents, depending on the potential harm that result from loss. This relates to their security classification and the volumes involved. Use a method that is appropriate for the type of information:

- For normal inter-office transit, use DX delivery services or agreed contracts for the movement of papers or files. Royal Mail letter post is otherwise acceptable for standard non-sensitive material, or letters at .
- The classification and any handling caveat such as be shown on the outer envelope. If the contents are sensitive, particularly if they contain personal details intended for an individual, the envelope be marked `ADDRESSEE ONLY`. Post rooms check addressee details, and open any envelope marked in this way.
- If more security is needed, either because material is being sent in bulk or the contents are more sensitive, tracked options including tracked DX or special delivery be used.
- Material marked be sent using any of the previous methods, with a return address and no protection marking on the outer envelope.
- Double enveloping might also provide additional protection, especially if there is a risk the package might burst or if it is being sent to a non- location where the `ADDRESSEE ONLY` instruction might not be recognised.

Confirming delivery

If you are sending sensitive or bulk information, you ensure that the recipient is expecting it and get confirmation of receipt. Consider a solution that allows you to track delivery. If you need to transfer or send personal data to or outside of the European area, discuss it first with the .

Faxing documents between sites

Office faxes only be used for transmission and exchange of information where other more secure means of communication, for example government email, are not possible.

Where use of fax machines (including Goldfax where available) remains the best option, it only be for information classified at and that is not especially sensitive. The reason is that fax material is sent over public networks. Faxed information might be individual items, including personal data.

Bulk transmission of personal data and information marked only be allowed following a risk assessment and approval from the Information Asset Owner.

The following controls and procedures also be applied by staff:

- Ensure that the recipient has a legitimate need to access department information for official business purposes.
- Take care to ensure that the correct number has been dialled, and that the authorised recipient is attending the receiving fax terminal at the time the information is being faxed.
- Immediately contact the authorised recipient to authenticate that they have received the information, verifying the quantity (the number of pages), and content of the information.
- If the recipient's fax line is busy and a transmission is not possible, wait until it is free. Do not leave the fax machine unattended. You confirm that the authorised recipient has received all the information.
- Each transmission should carry the following:
  - A unique reference number.
  - The identity of the originator.
  - The identity of the intended recipient.
  - A record of the number of pages transmitted.
- Ensure that the authorised recipient is aware of the handling requirements for information, including preventing information being viewed or accessed by unauthorised persons in their business.
- If the fax is configured to produce a confirmation of transmission report, including a copy of the first page of the transmission, ensure that you retain this hardcopy information and that it is not left on the fax machine where it might be seen by those who do not 'need to know'.

- Ensure that the fax is configured correctly, and that functions such as polling reception (programming to send messages to specific numbers), redirection, forwarding, and remote control are disabled.

Overview of threats and vulnerabilities

The public service telephone networks through which fax messages are transmitted are exposed to several significant security vulnerabilities and threats. These include:

- The potential that even UK to UK transmission is routed to overseas networks, increasing risks.
- Transmission within the UK may be intercepted at several places along the route.

In addition, the risks associated with fax machines are as follows:

- Unauthorised access to the built-in message stores to retrieve messages.
- Deliberate or accidental programming of machines to send messages to specific numbers.
- Sending documents and messages to the wrong number, either by misdialling, or by using the wrong stored message.
- Viewing of protectively marked messages by unauthorised persons, for example copies left unattended and unsecured on fax machines and traffic logs, and copies of fax messages retained on the machine's memory being accessed.

What to do if you think there has been a security breach

If you suspect that the security of the information you work with has been compromised in any way, you report it immediately. A security breach doesn't have to involve the actual loss of information. The potential loss of information also counts.

For example, if a security cabinet has been left unsecured, there might be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

The level of risk and potential impact to assets and most importantly physical harm to our people and the public determines the controls to be applied and the degree of assurance required. The ensure that a baseline of physical security measures are in place at each site, and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, for example in response to a security incident or a change in the Government Response Level.

The implementation of all security measures be able to provide evidence that the selection was made in accordance with the appropriate information security standards ISO27001/27002, and with Physical Security advice taken from the and (link is external).

The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested in order to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards are subject to annual review or more frequently if warranted.

Physical security advice

Physical security advice can be obtained by contacting .

Annex A: Suitable carriers

This guidance does not provide an exhaustive list of suitable carriers but does identify recommended options. The following notes provide further details.

Royal Mail

Ordinary letter post is acceptable for correspondence with members of the public or items that must be sent to private addresses. To prevent inappropriate opening of personal letters with sensitive personal data sent internally or to other business addresses, you mark the envelope 'addressee only'. This might also require double enveloping to protect the contents in transit, and prevent inappropriate opening on delivery.

Recorded delivery

Recorded delivery be used if the letter contains particularly sensitive information or identity documentation. The sender is given a reference and can confirm delivery and obtain a copy of the signature through the Royal Mail website.

Special delivery

This is similar to recorded delivery, but requires a named signature for receipt. Earlier delivery can be arranged (9am or 1pm). This service also allows online tracking of the item, suitable for more sensitive documents.

For more information, refer to the "Courier and postal services Royal Mail" document available on MyHub (log in to MyHub and use the search facility to locate the document).

DX

Ordinary DX services are acceptable for sending low volumes of files or enveloped papers between sites and other justice agency partners with registered DX addresses. When sending any volume or sensitive papers, managers ensure that the receiving office is expecting the delivery, and check receipt.

Tracked DX

This is recommended when a more formal tracking is required, either because of the volumes of files, or because they contain particularly sensitive case information.

There two further DX options which give added security:

- Courier Tracked.
- Secure DX.

For more information, refer to the "Courier Services Document Exchange and Next Day – DX Network Services" document available on MyHub (log in to MyHub and use the search facility to locate the document).

You can also use tracked courier services provided by FedEx.

Web Browsing

The provides access to the Intranet and Internet for business use. The access helps you to do your job effectively and efficiently.

security policies governs your use of these facilities.

Reasonable personal use is allowed, if:

- Your line manager agrees.
- It does not interfere with the performance of your duties.

You and your manager are responsible for ensuring that you use these systems responsibly.

If you connect to a website that contains unsuitable, illegal or offensive material:

- Disconnect from the site immediately.
- Inform your #unique_462.

The Department monitors the use of electronic communications and web-browsing activity. If your email use or web browsing seems unacceptable, your manager can request detailed activity reports.

What websites you can access

The 's approach to website access is continually reviewed and updated. By default, we try to allow access to as much as possible of the internet for all users. Inevitably, there are some restrictions, for the following reasons:

Cyber Security

- The site is an unacceptable security risk for systems or users. For example, sites known to host malware are blocked.

Technical

- The site causes technical issues which interfere with business activities. For example, a video site uses too much network capacity.

Business Policy

- Only a specific individual or group of users can access the site. For example, social media sites are blocked for systems or users in frontline roles.

The list of websites included in each of the categories is as small as possible. But if you cannot access a site that you think should be OK, you can request a review. Similarly, if you can access a site that you think should be blocked, request a review.

What to do if you are blocked from a website that you think should be OK

Log an incident with your #unique_462.

Provide the following details:

- The address of the website.
- The time you visited the site.
- The details of any block message that you received.

The will investigate the reason why you cannot access the website.

If there was a system error or fault, remedial action will restore access.

If the block is due to an access rule, the Security team reviews whether to change the rule.

What to do if you are able to access a website that you think should be blocked

Log an incident with your #unique_462.

Provide the following details:

- The address of the website.
- The time you visited the site.
- The reason why you think the site should be blocked.

Other help

- HMPPS Prison - All requests should be directed to the via a local or area IT Manager.
- HMPPS Probation - Log an incident with your #unique_462.
- All other teams, contact the .

Web browsing security policy profiles

There are two policy profiles, one for the Judiciary, and one for all other staff.

Each profile identifies categories of content that are normally blocked. Content that is not in a blocked category will normally be available to a profile.

Judiciary

All activity is logged. By default, no reporting takes place. However, reporting is permitted following appropriate judicial sanction.

The following categories of content are normally blocked for the Judicial profile:

- Advanced Malware Command and Control
- Advanced Malware Payloads
- Botnets
- Compromised Websites
- Custom-Encrypted Uploads
- Dynamic DNS
- Elevated Exposure

- Emerging Exploits
- Extended Protection
- Files Containing Passwords
- Keyloggers
- Malicious Embedded iFrame
- Malicious Embedded Link
- Malicious Websites
- Mobile Malware
- Newly Registered Websites
- Phishing and Other Frauds
- Potentially Exploited Documents
- Potentially Unwanted Software
- Security
- Sex
- Spyware
- Suspicious Content
- Suspicious Embedded Link
- Unauthorised Mobile Marketplaces
- User-Defined list

All other staff

Limited restrictions are in place to block web access. All activity is logged. Reporting is enabled for all activity.

The following categories of content are blocked for this profile:

- Adult Content
- Adult Material
- Advanced Malware Command and Control
- Advanced Malware Payloads
- Application and Software Download
- Botnets
- Compromised Websites
- Custom-Encrypted Uploads
- Dynamic DNS
- Elevated Exposure
- Emerging Exploits
- Extended Protection
- Files Containing Passwords
- Keyloggers
- Malicious Embedded iFrame
- Malicious Embedded Link
- Malicious Websites
- Mobile Malware
- Newly Registered Websites
- Phishing and Other Frauds
- Potentially Exploited Documents
- Potentially Unwanted Software
- Security
- Sex
- Spyware
- Suspicious Content
- Suspicious Embedded Link

- Unauthorised Mobile Marketplaces
- User-Defined list

Wifi security policy

Introduction

This policy gives an overview of wireless networking (wifi) security principles and responsibilities within the .

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.WIFI.xxx**, where **xxx** is a unique ID number.

Audience

This policy is aimed at:

Technical users	These are in-house Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
Service Providers	Any other business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services, including processing, transmitting,and storing data for, or on behalf of, the .
General users	All other staff working for the .

"All users" refers to General users, Technical users, and Service Providers, as defined previously.

Purpose

The purpose of this document is to define a set of security requirements for wifi networks, based on industry good practices and our local requirements.

POL.WIFI.001: Any exceptions to the policy be managed through the 's security risk management process.

Applicability

This policy applies to all owned or managed wifi networks provided for any purpose. It also applies to the use of third-party wifi networks by devices which handle information, for example staff end user computing devices.

wifi networks

POL.WIFI.002: Each wifi network have a defined policy which is reviewed at least annually, that describes:

- The purpose of the wifi network.
- The intended users of the wifi network.
- The Service Owner of the wifi network.
- The access controls that are applied to ensure that only those intended users can connect to the wifi network.
- User and administrator responsibilities for maintaining the security of the wifi network.
- Who has authority to expand or alter the wifi network.
- Logging and monitoring requirements and responsibilities for the wifi network.

General security requirements

The following statements apply to all -provided wifi networks.

POL.WIFI.003: Wifi networks be treated as extensions of trusted LANs or WANs.

POL.WIFI.004: Wifi networks be treated as untrusted bearers for the purposes of application security.

POL.WIFI.005: All products used in an wifi network support WPA2-Enterprise.

POL.WIFI.006: CCMP be used to protect the confidentiality and integrity of information transmitted over the wifi network.

POL.WIFI.007: Other wifi security modes (such as WEP) be enabled.

POL.WIFI.008: All products used in wifi networks support certificate-based authentication.

POL.WIFI.009: On wireless networks, isolation between wifi clients be enabled. Where there is no requirement for devices to communicate directly, isolation be enabled.

POL.WIFI.010: wireless networks use a DNS resolver that chains to the Protective Domain Name Service (PDNS) service.

POL.WIFI.011: All wireless networking equipment be kept patched and secure, whether connecting to wifi services or GovWifi.

POL.WIFI.012: All management of Wireless networking equipment be undertaken in compliance with the Privileged User Access Guide and any relevant Security Operating Procedures (SyOPS).

enterprise wifi networks

Note: enterprise wifi networks are those used solely for users and devices.

POL.WIFI.013: Pre-Shared Keys (PSKs) be used for user or device authentication.

POL.WIFI.014: PSKs be unique per user or device.

POL.WIFI.015: PSKs only be implemented with prior agreement from the cyber security team

POL.WIFI.016: PSKs be changed at least once a year.

POL.WIFI.017: EAP-PSK be used.

POL.WIFI.018: In higher-threat situations such as in a prison location where any unauthorised use of the Wireless network would constitute a security incident, mutually-authenticated authentication based on certificates be used.

POL.WIFI.019: EAP-TLS or EAP-TTLS be used.

POL.WIFI.020: Where user or device groups have differing functions, PKI trust domains be defined and used to maintain functional separation.

special-purpose wifi networks

POL.WIFI.021: If devices, including IoT or legacy devices, cannot meet the general security policy requirements, or if there are non-security reasons for segregating traffic onto different SSIDs, then dedicated wifi networks be created.

POL.WIFI.022: These dedicated networks have reduced authentication controls, for example a shared PSK or a reduced ability to rotate PSKs due to form-factor limitations.

POL.WIFI.023: In such circumstances, special care be taken to ensure that the general network architecture and other security controls constrain network connectivity for clients. The constraints limit network connectivity to the minimum required for them to function properly.

POL.WIFI.024: Other mechanisms such as MAC filtering be used to reduce the chance of misuse.

guest wifi networks

Due to complexities and management effort involved in running wifi solutions, the preference is to utilise the cross-Government GovWifi service: https://www.wifi.service.gov.uk/.

This also has the benefit of being available across HMG Departments and Agencies. GovWifi has a level of pre-registration, monitoring and filtering in place to protect the users. However, GovWifi does not provide enterprise level security functions. GovWifi users are required to maintain their own security controls. For users of GovWifi connections, this means using the -provided VPN services when accessing protected services.

POL.WIFI.025: Any considerations for not using GovWifi in an guest wifi network be discussed and agreed beforehand with the cyber security team.

POL.WIFI.026: Where GovWifi cannot be used, or where an existing guest wifi service exists,the following be in place:

- Regular rotation of the passphrase, with agreement from the . Normally, this requires a fresh and unique passphrase each day.
- Filtering and Monitoring for known 'bad-sites' and threats be in place at the network level.
- Guests wishing to utilise the service first register for access, and can then be provided with the passphrase for that day.

Logging and monitoring

POL.WIFI.027: Security monitoring for wireless networks be implemented, in accordance with the security monitoring policy.

POL.WIFI.028: Security logging be enabled to record activity such as client access events, authentication successes and failures, client association history, and relevant information about devices and users attempting to connect to the wireless network.

POL.WIFI.029: In higher threat environments, security logging also include identification of rogue access points, and logging of all attempted associations with the wifi network.

POL.WIFI.030: For guest wifi networks, but not including GovWifi, audit logs of sites accessed be retained for at least 6 months, including authentication details. This data is held to allow forensic analysis of data in the case of a security incident. No personal information except that required to conduct the analysis is logged or retained.

Using third-party wifi

POL.WIFI.031: staff ensure they have permission from the network owner before using wifi that is not operated by the .

POL.WIFI.032: Staff take reasonable precautions to check that their home wifi network is secure.

POL.WIFI.033: Staff use work-provided mobile phones to 'tether' their -provided devices for connectivity.

POL.WIFI.034: Tethered connections be password protected using unique and complex passwords.

POL.WIFI.035: Tethering passwords for devices be shared with non- users.

POL.WIFI.036: Public wifi networks or guest wifi provided at third-party sites only be used by devices which have suitable encryption for information. Here, 'suitable' means either an 'always-on full-take' VPN, or that provides appropriate application-level encryption for all services. This is currently (October 2021) limited to Dom1 and PTTP/MoJO laptops and mobile devices.

POL.WIFI.037: Staff travelling overseas follow the guidance on accessing IT systems from overseas regarding the use of wifi or other networks.

Enforcement

This policy is enforced by lower level policies, standards, procedures, and guidance.

Non-conformance with this policy could result in disciplinary action taken in accordance with the 's disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the department always cooperates with the relevant authorities, and provides appropriate evidence.

Information security incident management

Management of information security incidents and improvements

IT Security Incident Management Policy

How to use this policy

This policy is for all users and is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This policy describes what is needed to manage an IT Security Incident.

Information is listed beneath the following headings:

- Policy statements
- What is IT Security Management?
- Definition of an IT Security incident
- Types of incidents
- Incident detection and reporting
- Incident categories
- Escalations
- Incident management stakeholders
- Investigations
- System recovery
- Lessons learned

Security Team

In this policy, ' Security Team' refers to all the security teams within the .

The Security Team are responsible for:

- incident ownership, monitoring, tracking and communication
- sanctioning enhanced monitoring where appropriate
- updating the incident management database
- analysing security incidents as required
- initiating a forensic investigation
- providing progress reports to relevant parties

To contact the Security Team, send an email to .

Policy statements

This policy refers to the Policy Statements, **POL.IMP.001** to **POL.IMP.014**.

POL.IMP.XXX indicates the specific policy statement to be adhered to.

What is IT security management?

IT Security Incident management is the ability to react to IT security incidents in a controlled, pre-planned manner.

Preparation and planning are key factors to successful information security management. This policy sets out good practice for dealing with IT security incidents.

Definition of an IT Security Incident

A security incident is defined by the National Cyber Security Centre (NCSC) as:

- a breach of an IT system's security policy in order to affect its integrity or availability
- the unauthorised access or attempted access to an IT system

An IT incident may result in sensitive information being exposed, which might compromise business delivery or the Data Protection Act.

An incident might also cause harm or damage to individuals or organisations and result in operational disruption or reputational damage to the .

All staff be aware of the definition of a security incident and how to report it.

Incident Response

An incident response is the action taken when a security incident is detected or reported.

Responding to an incident requires informed decisions, taken as part of a consistent approach that is designed to reduce the consequences of the incident.

The process to respond to an incident be described in detail in an Incident Response Plan.

POL.IMP.001: Each IT system and service have an IT Security Incident Response Plan.

The IT Incident Response Plan and Process Guide has information on what to include in a Response Plan.

Types of Incidents

Types of IT Security related incidents include:

- breaches of the IT Security Acceptable Use Policy
- detection of malicious code such as viruses and malware
- network attacks or Denial of Service (DOS) attacks
- scanning and probing of a network, which might consume significant network resources
- the discovery of a new network vulnerability
- release of a patch or software update which is considered critical or an emergency
- a penetration test on a live operational IT system that reveals critical vulnerabilities
- unauthorised access to an IT system
- personal data incident due to accidental or deliberate loss or release of personal information
- any alert or activity report generated by an IT system that proves to be a real security alert

Incident Detection and Reporting

Security incidents may be discovered by:

- protective monitoring solutions
- incident reports by staff
- third-party reports to the
- breaches of IT Security Policy detected by an IT system
- data surrounding IT security incidents or suspected IT security incidents can be captured and monitored for suspected malicious activity or breaches of security

POL.IMP.002: All IT Security incidents or suspected incidents be reported to the IT Service Desk as soon as they are identified.

POL.IMP.003: All IT Security incidents involving personal data be reported to the Data Protection Team.

The Security Team is responsible for maintaining a database of IT Security incidents across IT systems.

This database contains:

- security incident reports
- the status of all reported security incidents and any actions taken to mitigate them

Further guidance on how to report a security incident.

Incident Categories

Security incidents are categorised to assess their impact and required level of escalation.

The three categories are:

- Low impact
- Medium impact
- High impact

POL.IMP.004: All IT Security incidents be categorised by the incident response team.

An IT incident may need to be recategorised if there are changes to the nature and impact of the incident.

Low impact incident

Low impact incidents are typically minor events such as a low-level breach in IT Security or a short-term loss of an IT service.

Medium impact incident

Medium impact incident are typically caused by:

- disregard for the IT Security Policy leading to a minor breach in security or the potential of data loss
- inappropriate use of IT assets
- theft or loss of data from an IT system that does not contain any personal information and is not protectively marked
- damage to an IT asset that impacts its usability
- connecting unauthorised equipment to an IT system
- prolonged or permanent failure of an IT system
- prolonged set of unsuccessful attempts to scan an IT network or instigate a denial of service attack
- a new critical security vulnerability in an IT system
- localised report of malicious code such as a virus on a terminal

High impact incident

High impact incidents require immediate escalation to the relevant Senior Information Risk Owner (SIRO), the Security Team, and the Data Protection Team if personal data is involved.

High impact incidents may require forensic investigation.

High impact incidents are typically caused by:

- malicious activity or espionage
- an incident that attracts media coverage
- intrusion into an IT network
- widespread malicious code attacks
- the theft or loss of personal or protectively marked data from an IT system

Escalations

If an incident needs to be escalated, it follow the chain of command through the incident response command structure.

The exact chain of escalation be outlined in the IT system's Incident Response Plan.

A typical command chain might be from the incident manager to the Major Incident Management team, to the relevant SIRO to Chief Security Officer (CSO) to Ministerial response.

Reasons for escalation might include:

- issues of national security
- if the incident is receiving media coverage
- if the incident has caused harm to a member of staff or public
- the has suffered reputational damage
- a requirement to report to another Department or central management function
- significant actual or potential loss of personal information where the Information Commissioner’s Office and Cabinet Office need to be informed

POL.IMP.005: Each IT Security Incident Response Plan include a pre-arranged escalation path, where each stakeholder is named and is aware of their role. Contact the Major Incident Management team if you need help creating documented escalation paths.

Incident Management Stakeholders

There are likely to be both internal and external stakeholders involved in incident management and response.

These will vary depending on the specific IT system or service.

POL.IMP.006: All staff report any actual or suspected incidents, including breaches of Security Policy, to their line manager and to the IT Service Desk.

POL.IMP.007: As part of operational readiness, Each SIRO ensure that each IT system or service under their remit has an IT Security Incident Response Plan. A guide for writing a plan is available in the IT Security Response Plan and Process Guide.

POL.IMP.008: All High impact IT Security incidents and any IT Security incident involving personal data be reported to the SIRO for your business area.

POL.IMP.009: All IT Security incidents involving the suspected or actual loss, theft, or compromise of an Information Asset be reported to the Information Asset Owner (IAO).

POL.IMP.010: If the IT Service Desk receives a report of a security incident, this be reported to the Security Team.

Investigations

The Security Team is responsible for the investigation of all IT Security incidents.

If legal or disciplinary proceedings require evidence to be gathered, a forensic investigation may be needed.

POL.IMP.011: The Security Team maintain documentation on investigations undertaken.

POL.IMP.012: Any investigation of an IT Security incident and the events surrounding it be reported to all relevant stakeholders.

System Recovery

Following an IT Security incident, the IT system, services or any compromised assets be restored to business as usual (BAU).

If IT systems or services are restored using backups, the systems or services being restored pre-date the incident and contain any weaknesses that could be exploited further.

POL.IMP.013: The IT Security Incident Response Plan show how an IT System or service will be restored or recovered following an IT Security incident. The method used to restore or recover an IT System be captured in the system's disaster recovery plan.

Lessons Learned

Once the cause of an IT Security incident has been identified steps be taken to make sure it will not happen again.

A report be prepared that describes:

- the incident
- the investigation
- the actions taken to restore the IT system or service to BAU
- all lessons learned

Lessons learned include action points on how to improve the business systems to reduce the likelihood of the incident re-occurring.

This report be sent to the SIRO who is responsible for forwarding it to all relevant stakeholders.

POL.IMP.014: For each Medium and High impact IT Security incident, a report be prepared, to include:

- a description of the incident
- a description of the incident investigation and its outcome
- mitigations and actions taken to resolve the incident
- any lessons learned and recommendations made

Lost devices or other IT security incidents

This guidance applies to all staff and contractors who work for the .

Related information

Laptops on page 73

What to do if your device is lost, stolen, or compromised

If data or information is lost or compromised, you should always report it as a data incident.

Note: You can help reduce problems by making sure that devices used for tasks are always shut down before leaving Government premises. Locking a laptop, or 'putting it to sleep' is not completely secure. A lost or stolen laptop can be accessed more easily if it is only locked or sleeping. A shut down makes sure that all security measures are in place, such as full disk encryption.

If you think your device is lost, stolen, 'hacked', or in some way compromised, you must:

1. Contact your . The analyst will ask the relevant questions and note responses on the ticket.
2. Tell your line manager as soon as possible.
3. For a lost or stolen device, contact the Police and make sure you get the incident reference number.

Summary

Find out more about how to report a security incident.

Information security aspects of business continuity management

Information security continuity

IT Disaster Recovery Plan and Process Guide

How to use this plan and process guide

This guide for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This plan and process guide is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This guide gives information on how to create and develop an IT Disaster Recovery Plan for your IT system or service.

The National Cyber Security Centre (NCSC) also offers guidance on how to effectively detect, respond to and resolve cyber incidents.

Business Impact Assessment

The service or system owner carry out a Business Impact Assessment (BIA) in order to:

- get an overview of the Business as Usual (BAU) functions for the IT system or service
- get an understanding of the business criticality of the service the IT system supports
- calculate a Recovery Point Objective (RPO), this is the maximum amount of data the business can afford to lose during a disaster
- calculate a Recovery Time Objective (RTO), this is the amount of time before the disaster begins to seriously impede the flow of normal business operations

Suggested content

Disaster recovery plans are specific to each individual IT system or service. They are intended to offer guidance to every listed role when responding to an incident.

When deciding the content of a Disaster Recovery Plan for an IT system or service, a useful start is to identify every potential disaster that may affect the system or service, together with procedures to resolve each one.

Each Disaster Recovery Plan include:

- the point at which the recovery plan be used

- a clear and detailed process to recover the IT system to BAU
- a list of key roles and a description of their responsibilities - each role have at least two sets of contact details
- a list of internal and external stakeholders to be contacted as soon as the incident happens, each stakeholder have at least two sets of contact details
- a communication list of everyone who needs to be contacted, together with the chains of communication that be followed
- a list of people who can undertake the role of recovery manager
- a series of steps to follow in order to mitigate the incident
- a list of criteria needed to initiate a forensic investigation, and the role(s) responsible for it
- clear instructions on how to escalate to a higher level of incident response, to include names and contact details and the reason for escalating the incident
- methods to maintain business continuity whilst the IT service is unavailable
- a process to identify and capture lessons learned during the incident
- the requirement for a written report for medium and high impact incidents

All plans be stored securely both online and offline. Roles and stakeholders mentioned in the plan know of its location and be able to access it.

Reviewing and testing

Disaster Recovery Plans be reviewed regularly, and updated if there have been any changes to systems or services, personnel, or communication chains.

Plans be tested and practiced regularly to help familiarise each of the roles with their responsibilities within the response process.

This is not an exhaustive list. If you need support in creating a plan, please contact the Service Operations Centre (SOC) and the Major Incident Team.

IT Disaster Recovery Policy

How to use this policy

This policy is for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This policy is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This policy describes what is needed to recover from an IT Disaster Event.

Information is listed beneath the following headings:

- Policy Statements
- What is an IT disaster event?
- What is IT disaster recovery?

- IT Disaster Recovery Plan
- Roles and responsibilities
- Planning
- Business Impact Assessment
- Testing and readiness review
- Reporting and alerting
- Recovery and review

Policy Statements

This policy refers to Policy Statements, **POL.ITDR.001** to **POL.ITDR.014**.

POL.ITDR.XXX indicates the specific policy statement to be adhered to.

What is an IT disaster event?

An IT disaster event is any incident that causes actual or potential loss of availability or integrity of an IT system, which results in the IT system being unable to function during business as usual (BAU) operations.

What is IT disaster recovery?

IT disaster recovery is the planned response to a disaster event which will restore an IT system to BAU operations.

IT Disaster Recovery Plan

An IT Disaster Recovery Plan lists the actions to be taken to recover an IT system from a disaster event, together with a list of key roles and their responsibilities.

POL.ITDR.001: Each IT system have an IT Disaster Recovery Plan.

The IT Disaster Recovery Plan and Process Guide describes the information to include in a Disaster Recovery Plan.

Roles and Responsibilities

POL.ITDR.002: All Disaster Recovery Plans contain an up to date list of roles and responsibilities.

Each role have a name, with at least two sets of contact details.

POL.ITDR.003: All staff who are listed in a Disaster Recovery Plan be aware of their role and its responsibilities.

The list of roles and responsibilities include internal and external stakeholders, together with everyone listed on the communications list.

The list of roles and responsibilities align with the Incident Management Plan (IMP).

A variety of individuals and teams may be responsible for business and IT service continuity, and escalation in case of a disaster. These may include:

- Executive Committee
- Senior Information Risk Owner (SIRO)
- Chief Security Officer (CSO)
- Information Asset Owner (IAO)
- Service Operations (SO), which includes the Major Incident Management Team and the Security Operations Centre (SOC)
- IT Service Continuity Management

A Disaster Recovery plan include the relevant escalation process through the teams and individuals listed for each IT system.

Planning

An IT Disaster Recovery Plan supports the decisions and steps taken to reduce the effects of disasters and identifies the steps needed to recover IT systems back to BAU.

An IT Disaster Recovery Plan :

- contain identified risk scenarios and strategies to recover from them
- describe the circumstances in which the plan is invoked.

Business Impact Assessment

A Business Impact Assessment (BIA) be undertaken to identify the key disaster recovery requirements of the assets, services, and business processes supported by a specific IT system.

The BIA contain:

- a Recovery Time Objective (RTO): the time between a disaster event occurring and full IT systems and services being restored
- a Recovery Point Objective (RPO): the period of time during which the business can tolerate data loss

POL.ITDR.004: A Disaster Recovery Plan contain an RTO and RPO. The plan may contain more than one of these depending on the system.

POL.ITDR.005: Any disaster recovery action ensure that the IT system can recover from a disaster within the RTO recorded in the BIA.

POL.ITDR.006: Any disaster recovery action ensure that the IT system can recover from a disaster within the RPO recorded in the BIA.

Testing and Readiness Review

An IT Disaster Recovery Plan be tested regularly to ensure that:

- the plan remains fit for purpose
- the plan reflects all changes in personnel and updates to system information
- everyone with a role in the plan knows their responsibilities

POL.ITDR.007: Each IT system have its IT Disaster Recovery Plan tested before commencing live operations.

POL.ITDR.008: All IT Disaster Recovery Plans be tested at least annually, and after significant update to an IT system. The testing schedule be outlined in the IT Disaster Recovery Plan.

POL.ITDR.009: The IT Disaster Recovery Plan be reviewed after each test and updated as required to ensure it is fit for purpose.

POL.ITDR.010: Each IT Disaster Recovery Plan define the circumstances when the plan is to be invoked.

Reporting and Alerting

The reporting and alerting structure of an IT Disaster Recovery Plan align with that of the corresponding IT Security Incident Response Plan.

Every stakeholder that needs to be informed, be listed as a key contact within the plan.

POL.ITDR.011: The reporting and alerting structure within an IT Disaster Recovery Plan align with the relevant IT Security Incident Management Plan and Business Continuity Plan. Responsibility for business continuity resides with the SO.

Recovery and Review

The process to recover from a disaster event ensure that security vulnerabilities are not introduced or re-introduced during the restoration process.

POL.ITDR.012: Each IT Disaster Recovery Plan contain pre-defined and tested processes and procedures to restore an IT system or services, which has been disrupted or disabled during a disaster event.

POL.ITDR.013: Each Disaster Recovery Plan describe in detail the procedures to enable an IT Security System return from recovery mode to BAU.

Lessons learned be collated in an after-action report and be fed back to appropriate stakeholders.

POL.ITDR.014: Following a disaster incident, an after-action report be produced, which contains:

- all lessons learned
- actions to be taken to update processes and plans

IT Investigations - Planning and Operations Policy

How to use this policy

This policy is for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This policy is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

Policy Statements

This policy refers to Policy Statements, **POL.POP.001** to **POL.POP.015**.

POL.POP.XXX indicates the specific policy statement to be adhered to.

IT Forensics

IT forensics is the collection, storage, analysis and preparation of digital evidence that might be required in legal or disciplinary proceedings,

Data used in a forensic investigation be collected, preserved and analysed using systemic, standardised and legally compliant methods.

This will ensure that data gathered is admissible as evidence in a legal case, dispute or disciplinary hearing relating to an IT security incident.

There are two types of forensic investigation:

- proactive forensic monitoring - as part of an indentified security control
- reactive investigation - where a suspicious incident has been identified or reported

A forensics investigation be carried out:

- if an area needs proactive monitoring to enable forensic investigation
- if a business function makes a request via incident management escalation channels, to gather forensic evidence.
- if an investigation is requested as part of the IT security incident management process
- if requested as part of a leak investigation.

POL.POP.001: Each IT system or IT domain be covered by a Forensic Readiness Plan.

POL.POP.002: Each Forensic Readiness Plan include:

- an assessment of the risk management benefits
- authorisation from the IT Security Team and Senior Information Risk Officer (SIRO)

- a corresponding IT security incident management plan

Risk management benefits include risk assessments and cost-benefit-analysis, which will determine if an investigation is viable from a risk and cost perspective.

POL.POP.003: Forensic investigations in support of leak investigations be requested by the individual responsible for the leak investigation.

Integrity of Digital Evidence

POL.POP.004: Each forensic investigation be guided by the principles set out by the ACPO guidelines issued by the National Police Chiefs' Council (NPCC).

The integrity of data, which subsequently relied upon in court, be maintained throughout the forensic investigation process.

Any person accessing data as part of an investigation be competent to do so and able to justify the relevance and implications of their actions.

Each investigation be documented clearly and leave an audit trail that will enable a third-party to examine each process and replicate the findings,

The person leading the investigation is responsible for ensuring that all methods used are carried out in accordance with the law.

Investigations be conducted in line with policies.

Evidence Collection and Storage

Security teams be able to monitor systems to detect and respond to potential security incidents. If an incident needs to be investigated further, forensic tools be used to assess and gather evidence.

The Forensic Investigation Owner (FIO) is responsible for the collection and management of digital evidence.

An external organisation conduct the investigation on behalf of the .

Each item of evidence collected be managed according to the relevant Forensic Readiness Plan.

POL.POP.005: Each Forensic Readiness Plan include a process for the collection and storage of digital evidence, to include provision for where this task is conducted by an external organisation.

POL.POP.006: All users of an IT system be made aware that their access is monitored, and that IT forensic techniques be used to capture evidence as part of an investigation into an IT security incident.

POL.POP.007: A Forensic Readiness Plan contain clearly defined procedures and methods for conducting a forensic investigation. The be able to resume business operations following an IT security incident. Any forensic investigation be conducted in a manner that enables the restoration of IT services.

POL.POP.008: A Forensic Readiness Plan consider business continuity arrangements to ensure that essential functions are able to be restored. Digital evidence be handled carefully in order for it to remain admissible.

POL.POP.009: Each forensic investigation have a clearly documented chain of custody for all digital evidence.

POL.POP.010: The Security Team is responsible for the integrity of digital evidence. Each forensic investigation have a named FIO who is responsible for the investigation and management of digital evidence.

POL.POP.011: Any investigative action taken on a piece of evidence be captured and recorded. This record include details of the action taken and the person responsible for undertaking that action.

POL.POP.012: Admissibility of evidence in a court of law depends on how the evidence was captured. Before capturing any evidence, advice be sought from the legal team and forensic investigation provider.

POL.POP.013: Each Forensic Readiness Plan include details of how to securely dispose of evidence when it is no longer required. This conform with Secure disposal of IT equipment.

Legal Requirements

Investigations of electronically stored information within the conform to the latest legal and regulatory guidelines.

BS 10008:2022 provides information on the collection of electronically stored information as evidence.

POL.POP.014: During each forensic investigation, methods used to capture digital evidence be in accordance with BS 10008:2022.

Reporting and Communication

Each IT Security Incident Management Plan contains a communication plan and an escalation plan that be followed when responding to an IT Security incident.

The IT Security Incident Response Plan and Process Guide gives more information.

For major incidents it might be necessary to consider escalating the forensic investigation process to an external body. This might be:

- Law Enforcement
- National Cyber Security Centre (NCSC)
- Cabinet Office
- legal advisors
- Other Government Agencies as required

POL.POP.015: Each Forensic Readiness Plan include the reporting structure and escalation path for internal and external teams and the individual responsible for managing the incident. This be consistent with the corresponding IT Security Incident Response Plan and Process Guidea. The forensic investigation process enable the chain of evidence to be passed to outside agencies, if required.

IT Security Incident Response Plan and Process Guide

How to use this guide

This guide is for all users and is part of a set of policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This guide gives information to help create and develop an IT Incident Response Plan for your IT system or service.

The also offers guidance on how to effectively detect, respond to and resolve cyber incidents.

Suggested content

Incident response plans are specific to each individual IT system or service.

When deciding what should go into an Incident Response Plan for an IT system or service, a useful start is to identify every potential incident that might affect the system or service, and list the ways to resolve each one.

Each Incident Response Plan include:

- a list of key roles together with a description of their responsibilities - each role have at least two sets of contact details
- a list of internal and external stakeholders to be contacted as soon as the incident happens, each stakeholder have at least two sets of contact details
- a communication list of everyone who needs to be contacted, together with the chains of communication that be followed
- a list of people who can undertake the role of incident manager

- a series of steps to follow in order to mitigate the incident
- a method to identify the need for forensic investigation, and the role responsible for invoking it
- clear instructions on how to escalate to a higher level of incident response, to include names and contact details and the reason for escalating the incident
- a detailed process to recover the system to business as usual (BAU)
- a process to identify and capture lessons learned from the incident
- the requirement for a written report for medium and high impact incidents

All plans be stored securely both online and offline. Roles and stakeholders mentioned in the plan know of its location and be able to access it.

Incident response plans are intended to be flexible guides to help every role listed to respond to an incident.

Reviewing and testing

Incident Response Plans be reviewed regularly, and updated if there have been any changes to systems or services, personnel, or communication chains.

Plans be tested and practiced regularly to help familiarise each of the roles with the response process.

This is not an exhaustive list. If you would like support in creating a plan, please contact the Service Operations Centre (SOC) and the Major Incident Team.

Compliance

Compliance with legal and contractual requirements

Data security and privacy

Data Security and Privacy

We believe that our technology must keep data safe and protect user privacy.

Our digital projects contain important information. Serious data breaches might result if we fail to:

- protect information
- handle it correctly at all times
- dispose of it safely when it is no longer required

Breaches might cause:

- harm to individuals
- financial loss to the
- a loss of confidence in us as an organisation

For personal data, the EU General Data Protection Regulation (GDPR) and UK Data Protection Act (2018) apply. These make the consequences of data breaches very clear.

To follow the data regulation/legislation, we **must** ensure that:

- we protect data to the best of our organisation's capabilities
- we collect data only for described, lawful purposes
- we use data only for the described, lawful purposes

Why are security and privacy important?

Breaches can have an adverse effect the relationship between citizen and government.

Not only do we have a duty to protect citizens data, but the penalties for violations are also severe. Under the GDPR, serious infringements can result in fines of up to €20M.

We must apply appropriate security and privacy protection to all the information we hold and process, at all times.

We should treat all data as sensitive unless proven otherwise.

All our work must follow this ethos.

When this applies

This principle applies to **all** technology projects and business activities.

While GDPR applies only to personal information, all projects and tasks must have excellent data security and privacy characteristics. If they handle personal data, they must do so correctly. Projects must follow guidelines unless exceptional and approved circumstances apply.

The Information Commissioner's Office (ICO) - the UK's independent regulatory office for data protection - has published guidance on how to determine what is personal data.

A Data Protection Impact Assessment (DPIA, formerly commonly known as a Privacy Impact Assessment or PIA) is required for all projects. There are some exceptions described by the ICO.

Data privacy

The provides services, guidance, and support for all aspects of data privacy and protection.

For example, they have protocols and procedures to help ensure acceptable use of personal information.

Risk Assessment Process

Risk Reviews

Information and the supporting processes, systems and networks are important and valuable assets. They are central to enabling the to perform its functions and provide services to the public, the legal professions, and other government departments and organisations.

Confidentiality, integrity and availability of information is essential to maintain the 's ability to provide efficient and effective services, maintain compliance with legal and regulatory requirements, and maintain its and the Government's reputation.

The and its information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, fire and flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

The 's dependence on its information systems and services means that there is always a possibility of technology-enabled security threats. Connections between the 's computer networks and public and other private networks, and sharing of information resources, further increase the difficulty of achieving and maintaining control.

It is essential that the identify its information security requirements. There are three main sources of these requirements.

- The legal, statutory, regulatory and contractual requirements that the , its partners, contractors and service providers have to satisfy.
- The principles, objectives and requirements for information processing that the and Government have developed to support their operations, for example the protective marking system and government baseline security standards.
- Assessed risks to the . Through risk assessment, threats to assets are identified, the potential business impacts of these threats are estimated, and the vulnerability to and likelihood of occurrence of the threats are evaluated.

Assessing information security risk

Security requirements are identified by a methodical assessment of security risks. Expenditure on security controls needs to be balanced against the business harm likely to result from security failures. Risk assessment is systematic consideration of:

- The business harm (the 'impact') which is likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.
- The realistic likelihood of such a failure occurring in the light of the threats to and vulnerabilities of the system, and the controls currently implemented.

Managing information security risks

The results of the risk assessment are identified risks and risk severities. These help guide and determine the appropriate management action, and priorities for managing information security risks. Risks with a high severity level would justify the expenditure of more resources to control them than risks with a low severity level.
Risk Management involves identification, selection and implementation of justified security and contingency 'countermeasures' to reduce risks to an acceptable level.

Countermeasures can act in different ways such as:

- Reducing the likelihood of attacks or incidents occurring.
- Reducing the system's vulnerability.
- Reducing the impact of an attack or incident should it occur.
- Detecting the occurrence of attacks or incidents.
- Facilitating recovery from an attack or incident.

Risk management requires a judgement about what is an acceptable level of risk. Although this is a business decision, it does require a thorough understanding of the nature of the risk and the effectiveness of the countermeasures implemented to manage the risk. For some systems or scenarios, specialist advice might be needed.

When taking risk management decisions, consideration must be given to the full implications of the decisions taken. Failure to implement some countermeasures might breach legal or regulatory requirements. This is unlikely to be an acceptable risk management decision. Failure to meet other countermeasures might breach Government information security standards; as a consequence it might not be possible to link the system with other systems. This might limit the usefulness of the system.

Consideration must also be given to what are tolerable financial losses, political sensitivities and adverse publicity. The cumulative effect of accepting high levels of risk should also be taken into account.

Information security in projects

Information security controls are considerably cheaper and more effective if incorporated at the system requirements specification and design stage. Information risk assessments must be part of the project process.

Ongoing information security risk management

Effective risk management does not end once a risk assessment has been done and the required countermeasures implemented. Checks need to be carried out to ensure that the countermeasures are being applied effectively. It is also important to carry out periodic reviews of security risks and implemented controls to:

- Take account of changes to business requirements and priorities.
- Consider new threats and vulnerabilities.
- Confirm that controls remain effective and appropriate.

The role of security in risk assessment and risk management

The security team can provide help in all areas of security risk management for systems. Examples include:

- Advice on risk assessments.
- Help with carrying out risk assessments.

- Assist with the risk management decision process.
- Help with creating and managing documentation compliant with standards.
- Assisting with mandatory Government risk assessments.
- Advice on compliance checking.

Glossary and Acronyms

Glossary

This information is a reference list of terms and abbreviations.

The NCSC has a comprehensive cybersecurity glossary available on its website.

Terms

2FA

Refer to Multi-factor authentication.

Authorised User

Any user of services covered as authorised by the .

Blue Team

The internal security defence team in an organisation. Within the , this work is performed by the Security Team.

Brute Force Attack

The application of lots of computer power, to try and perform a task using a huge number of values. Typically used to try out many passwords, to gain access to systems.

Business Continuity Plan (BCP)

A document that outlines the procedures in place for a business to continue to operate, despite an unexpected disruption to services. These disruptions might be things such as cyber attacks, pandemics, or natural disasters.

Credentials

Information used to prove someone's identity, to confirm that they really are who they say they are. Typically includes passwords, tokens, and certificates.

Critical infrastructure attack

Critical infrastructure refers to the physical and cyber structures, facilities, and systems that are essential for a country to function. Attacks on these resources would harm the physical security, economic security, or public health of the country.

Customer

Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. The term customers is also sometimes informally used to mean users, for example "this is a customer focused organisation".

Dark web

Generic name for encrypted online content that is not indexed by search engines. The information is only accessible with special software or tools.

Data breach

An incident where data is accessed in a non-authorised way.

Decryption

The reverse of an encryption process.

Distributed Denial of Service (DDoS) attack

Legitimate users cannot access computer services, because threat actors are overloading the service with requests. Also referred to as a Denial of Service (DoS) attack.

Digital footprint

A collection of data and information traces left behind by a user, as they do activities online. For example, all the things you've ever searched for on Google.

Double encryption ransomware

Refer to ransomware.

Encryption

The process of converting human-readable text into unreadable 'disguised' information, or 'ciphertext'. You can see it, but you can't understand it. Only someone with a decryption key can convert ('decrypt') the unreadable information back into human-readable form again.

Exfiltrate

The formal name for a technique used by threat actors and malware to surreptitiously copy and transfer data out of a system. This is data theft.

Exploit

A program or process that takes advantage of a vulnerability in a system to cause system problems, or to access or modify information without authorisation.

Incident

Any event which is not part of the standard operation of a service, and which causes, or might cause, an interruption to, or a reduction in, the quality of that service. A breach of the security rules for a system or service.

Incident Management

The process responsible for managing the lifecycle of all incidents. The primary objective of incident management is to return the IT service to users as quickly as possible.

Insider threat

Any threat from current or former employees of an organisation who have inside information or authorised credentials that might be used to cause harm to the organisation, accidentally or maliciously.

Macro

A small program or script that automates tasks in an application, such as Microsoft Office. Might be used by attackers can use to gain access to, or harm, a system.

Malware

Malicious software. This includes things like viruses, trojans, worms, or any code that can have a negative impact on an a system.

Multi-factor authentication (MFA)

Use of two or more different components to verify a user's claimed identity. Typically an extra component, in addition to a password. MFA often uses an authenticator app or SMS text to deliver a single use code. Also Two-factor authentication (2FA).

Open Source Intelligence (OSINT)

Information gathered from public information. This includes data from social network accounts, company websites, and other openly available information sources.

Operational Security Team (OST)

Deprecated name for the Security Team within the . The Security Team help protect against cyber attacks, and help manage incidents. Sometimes referred to as the Blue Team. They can be contacted through email: .

Out of band check

An additional check performed using a different communication channel, to verify identity or intent. The check helps prevent phishing or social engineering attacks. For example, if you receive an email from a senior manager, asking you to perform an unusual task, you should want to check that the request is genuine. If you reply by email to the original request, that's an 'in band' check, and can't be trusted, because it's possible the manager's email has been compromised. But if you called the manager by mobile phone to check the request, that's using a different communication technology, so it's an out of band check. A threat actor would have to compromise both the manager's email and their mobile phone account to succeed in tricking you. For more detail on out of band checks, refer to this additional information.

Password

A secret string of characters, numbers, and often symbols. When used with a valid user ID, a password enables access to an account.

Patching

Applying updates to software or firmware to improve security and enhance functionality.

Phishing

Untargeted mass emails sent to many individuals. The email typically asks for sensitive information, or encourages you to visit fake websites, or to send money. For more information, refer to the phishing guide.

Problem

A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation.

Problem Management

The process responsible for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening, and to minimise the impact of incidents which cannot be prevented.

Process

A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process might include any of the roles, responsibilities, tools, and management controls required to deliver the outputs reliably. A process might define policies, standards, guidelines, activities, and work instructions if they are needed.

Ransomware

Malicious software that makes data or systems unusable by encrypting it and then demanding a payment from the victim to decrypt it. Double Extortion Ransomware exfiltrates the data before encryption and demands a ransom payment to stop the threat actor releasing the data to the public, as well as for decrypting the system.

Red team

This is an internal or external team that tests organisational security by simulating cyber attacks as realistically as possible. Together with the Blue Team, the team helps to improve the cyber defences of the organisation.

Resolution

Action taken to repair the fundamental cause of an incident or problem, or to implement a workaround.

Resolver Group

May include a wide range of IT teams, including support and development personnel, other Service Management Functions (SMFs), other units within the organisation, outsourcing providers, partners, and other third parties.

Service Desk

The single point of contact between the service provider and the users. A typical Service Desk manages incidents and service requests, and handles communication with the users.

Social engineering

Manipulating people into doing things or divulging information that is of use to a threat actor.

Tabletop

An exercise created to try out Business Continuity Plans (BCPs). These exercises create realistic scenarios, and play through a number of obstacles, to ensure organisations have robust BCPs.

Tailgating

An unauthorised individual forcefully or stealthily gaining access to a building, typically by entering immediately behind an authorised user.

Threat actor

A general term that encompasses all types of individuals and groups that use cyber methods to cause harm. This includes competitors seeking to steal information, cyber criminals attacking for political or monetary gain, accidental or malicious insider threats, spies, social and political activists, and assorted hackers.

Trend Analysis

Analysis of data to identify time related patterns. Trend analysis is used in Problem Management to identify common failures or fragile configuration items, and in Capacity Management as a modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.

Virtual Private Network (VPN)

An encrypted network created to allow secure connections for remote users.

Vulnerability

A weakness in software, a system, or process. A threat actor might seek to exploit a vulnerability to gain unauthorised access to a system.

Zero day (0day)

A vulnerability in a system that few people know about. threat actors can exploit an 0day to attack or affect data and systems.

Zero trust

The assumption that all requests and connections are potential breaches, and so must be verified and authenticated before being allowed.

Out of band checks

An out of band check is when an individual uses a different method of communication than the one the message came from. This method means that if one communication method is compromised, you quickly find out by using a different communication method to confirm validity. The likelihood of multiple communication methods for the same person or team being compromised is low.

Out of band checks are an easy method to confirm the legitimacy of communications and requests. They can confirm the identity behind a message or request, and they can confirm the validity of the message or request itself. Social engineering techniques and phishing tactics take advantage of people who do not use out of band checks. By doing an out of band check, these sorts of attacks can be stopped very easily.

Example 1: You receive an email request for an urgent review of an invoice, and immediate payment. The email comes from someone unexpected. You should find the official contact details of that person, and contact them using a phone call - but not email - to confirm that they did indeed send the original email. If they did send the email, you can proceed with the request. If they did not send the email, you can report the email as a phish, and also alert the owner of the email address that their email address might have been compromised.

Example 2: You receive a phone call from someone claiming to be your bank, or HMRC, or HMCTS. You hang up the call, and locate the official website for the company. You should be able to find multiple official contact details there. Use one of these to contact the place the caller claimed to be from. If, for example, the claim was that your bank was calling, you can call the direct number and speak to the switchboard about the reason for the initial call. They will forward you to the correct department. You can then confirm the validity of the original call, and so confirm whether the original caller was actually from your bank or not.

Example 3: Someone enters your place of work, and claims to have a meeting with a specific person. Unfortunately, there is no record of this on the expected visitor list. You can call or email the person within your place of work to confirm the visitor is legitimate. This check also works if tradespeople arrive unexpectedly, because you can contact both the relevant person within your place of work and also contact the company they claim to be from, using the company's official website contact details.

Example 4: You receive an email requesting that you reset your password immediately. The email contains a link to perform the password reset. You have not attempted to login to that account recently. You should use an internet search for the website or type the URL directly if you know exactly what it should be. When you attempt to login, the website will let you know if you need to reset your password. If not, you know someone else has attempted to gain access to your account. That would mean the password reset request was not legitimate, and most likely a phishing attempt hoping to get your username and password through the reset link in the original email. Similarly, if you get an MFA request unexpectedly, do not confirm it unless you were indeed attempting to access that account immediately before the request came through. If you get an MFA request, but had not been trying to connect using the account, you should change the account password as soon as possible, because it might have been compromised.

When doing an out of band check, be sure to pick a different method of communication to the one used to contact you originally. If someone emails you unexpectedly, perform an out of band check by making a phone call. If someone calls you, perform an out of band check by using the Internet. It is very unlikely that multiple communication channels have been compromised.

Be sure to get official contact details for companies only from their official websites. Never be afraid to hang up on someone and check their identity through another method, especially if they are asking for sensitive or personal information or credentials. Never be afraid to check the legitimacy of unusual email requests. by contacting the sender through a different communication channel.

Doing an out of band check lets you confirm that the messages come from the person they claim to be, and that the requests are valid. This helps prevent you or your company from losing money to fake invoices, from accidentally giving up sensitive information or credentials, and from having unauthorised individuals in your place of work. Doing an out of band check is fast and easy.

All members of your workplace should be happy to receive such a check. It shows that you take security seriously, and that you are helping to protect them as well as yourself.