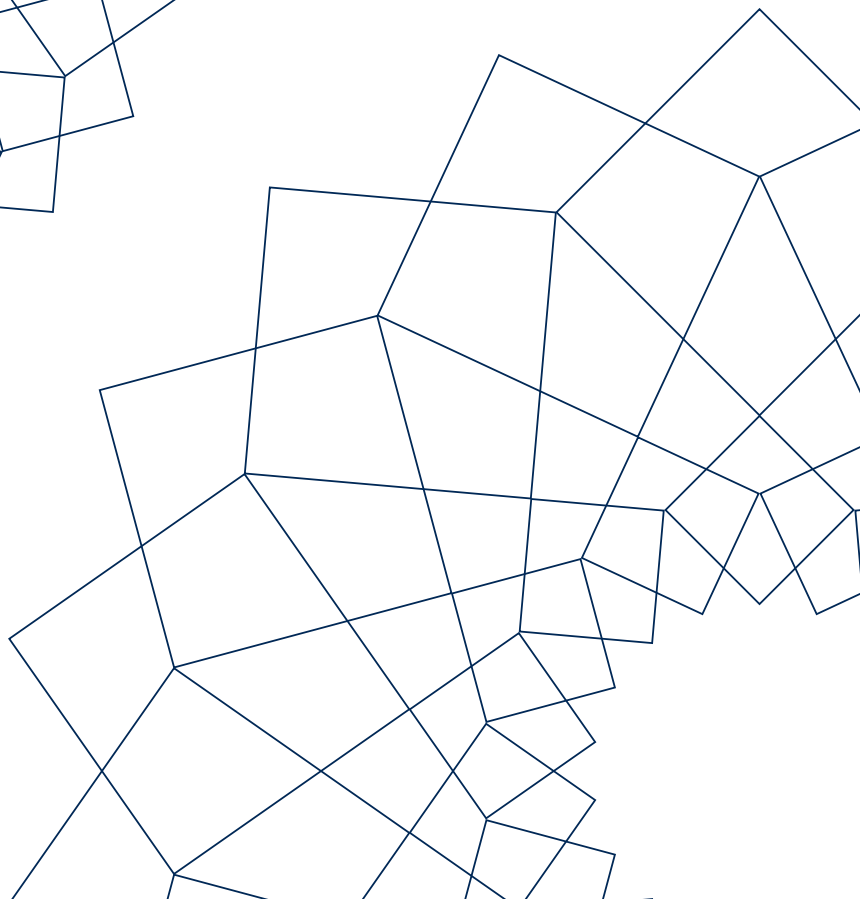
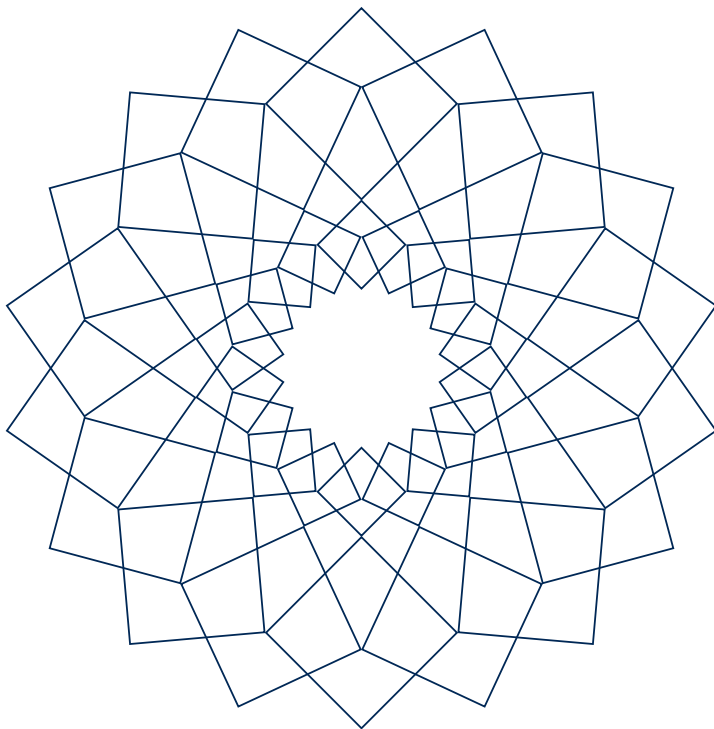




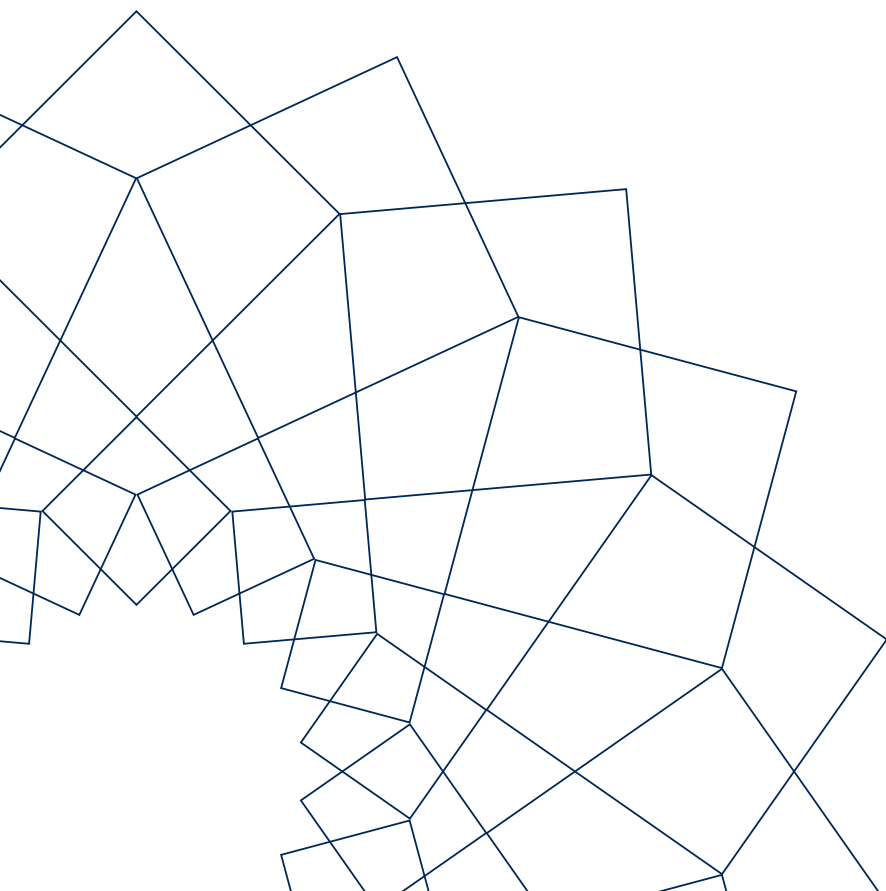
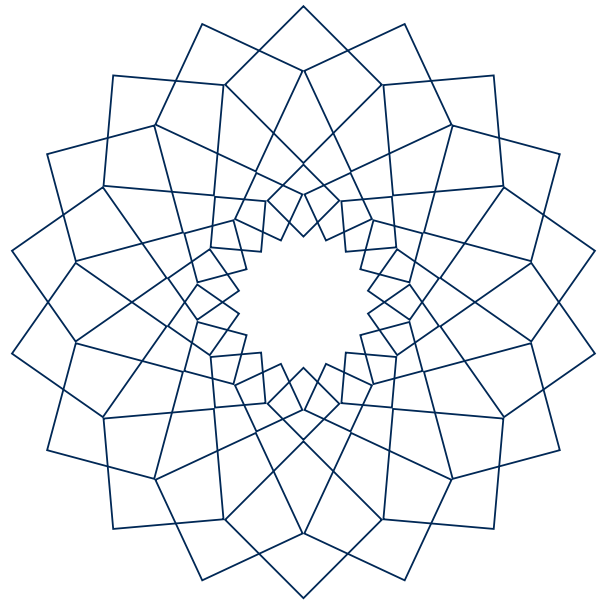
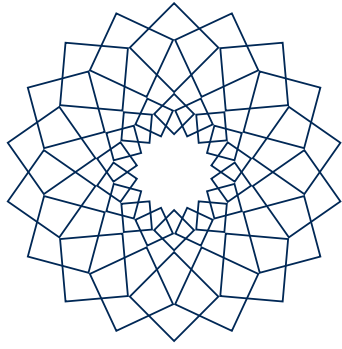
Ministry
of Justice

MoJ ICT Security Guide



Moj ICT Security Guide

June 2014



Contents

1. Introduction	3
1.1 What is ICT Security	3
1.2 About this guide	3
1.3 Who needs to read this guide?	4
1.4 Why you need to read this guide	4
2. ICT Security Policy	5
2.1 ICT Security Policy framework	5
2.2 ICT security policies	5
2.3 Privacy	6
3. ICT security infrastructure	7
3.1 ICT security management	7
4. Information Security	10
4.1 Government Security Classification of MoJ systems	10
4.2 Passwords	10
4.3 Access control	11
4.4 Back-ups	11
4.5 Information exchanges and data downloads	11
4.6 Removable media	12
4.7 Secure deletion and disposal	12
5. ICT Security Incidents	13
5.1 What is an ICT security incident?	13
5.2 Reporting ICT security incidents	14

6. Malicious software	15
6.1 Malicious software	15
6.2 Sources of malicious software	15
6.3 Prevention of malicious software	16
6.4 Responding to malicious software	16
7. Electronic Messaging	17
7.1 Risks of using electronic messaging	17
7.2 Using electronic messaging	18
7.3 Criminal Justice Exchange (CJX)	19
7.4 Criminal Justice Secure Electronic messaging (CJSM)	19
7.5 Additional measures for secure electronic messaging	20
7.6 Using CJSM securely	20
8. Intranet, GSi and the Internet web sites	21
8.1 Intranet and GSi web sites	21
8.2 Internet world wide web	21
9. Other Internet services	22
9.1 Web-based email	22
9.2 Bulletin board and groups	22
9.3 Social networking	22
9.4 Data and File transfers	23
10. Passwords	24
10.1 Password policy	24
10.2 Choosing a good password	25

1 Introduction

In this section

- What is ICT security?
- About this guide
- Who needs to read this guide?
- Why you need to read this guide

1.1 What is ICT security?

Ministry of Justice (MoJ), is dependent upon computers to store, process and communicate information. Information Communication Technology (ICT) security is primarily concerned with maintaining the security of this information. Information is an important business asset and is valuable to MoJ; consequently it needs to be suitably protected from a wide range of threats, in order to ensure business continuity, minimise business damage and protect personal data. Information communication technology security is characterised as the preservation of:

Information communication security is characterised as the preservation of:

- confidentiality: ensuring that information is accessible only to those authorised to have access;
- integrity: safeguarding the accuracy and completeness of information and processing methods; and
- availability: ensuring that authorised users have access to information when required.

The computers on which MoJ's business systems depend are also important business assets with a value of their own, separate to the value of the information they hold, and are particularly vulnerable to loss and damage. Computers are usually high value, attractive to thieves, often easily carried, concealed and damaged.

1.2 About this guide

This guide gives you advice and guidance on the main security issues that are likely to affect you as a computer user within MoJ, including its Agencies and Associated Offices. It also sets out your individual responsibilities for ICT security.

1.3 Who needs to read this guide?

This guide applies to all users of computer systems processing Moj data, including staff working in its Agencies and Associated Offices, contractors, agency and casual staff and service providers' staff. For brevity, these users will be referred to as staff or employees within this guide. All Moj employees must ensure that they are familiar with the contents of this guide and be aware of and comply with Moj's ICT Security Policy and procedures. Members of the judiciary who use computer facilities provided by Moj should additionally refer to any separate security guidance provided for the judiciary.

1.4 Why you need to read this guide

1.4.1 Legislation

You must adhere to legal and regulatory obligations in order to protect both yourself and Moj's assets. Failure to do so may result in criminal or civil proceedings being taken against you or Moj.

1.4.2 Government policy and standards

The guide is based upon HMG security policy produced by the Cabinet Office and applicable to the Home Civil Service as well as other organisations. HMG security policy is supported by standards and guidance produced by CESG. CESG is a division of GCHQ and is the UK Government's National Technical Assurance authority for Information Assurance. HMG security policy is aligned with, and supports conformance to, the Standard for Information Security Management – the ISO/IEC 27000 family of standards. The ISO/IEC 27000 series includes standards on information security management system requirements, risk management, metrics and measurements and implementation guidance.

1.4.3 Financial and operational impact and Ministry of Justice's reputation

Moj can suffer financially due to:

- compensation claims: if it breaches any regulatory or legislative requirements, Moj could incur financial penalties;
- theft: of ICT equipment and information held on it;
- fraud: some of Moj's computer systems are concerned with payments to suppliers and court users – if the use of these computers is not controlled, Moj runs the risk of fraud against it; and
- recovery costs: lost information will need to be recovered – there will usually be a price to pay for this, either in payments to suppliers or overtime payments to staff.

Moj can suffer operationally due to:

- operational disruption of Court proceedings;
- accidental premature release of a prisoner.

Ministry of Justice's reputation could also suffer as a result of the bad publicity.

2 ICT Security Policy

In this section

- ICT Security Policy Statement
- Privacy expectations
- Policy and guide review

2.1 ICT Security Policy framework

Moj's ICT security policy forms part of Moj's corporate security policy.

- Corporate security policy

IT systems are crucial in delivering the Department's core business activities effectively and all staff are required to understand their obligations in how to safeguard Moj data and how to use IT appropriately.

The ICT security policy framework is designed to;

- inform you on the acceptable use of Moj ICT
- let you know how to safeguard information assets from unauthorised access and modification
- describes how you should use, access and disclose information in accordance with security classification policies, regulations and applicable legislation
- allows the department to detect, manage and recover from security incidents with the least disruption to the organisation
- ensure Moj IT suppliers and service providers comply with the minimum requirements set out in this policy and within the wider security policy framework
- ensure that Moj information and IT assets are utilised for Moj business use only
- enable Moj to make best use of its investment in IT

2.2 ICT security policies

- [ICT security policy](#)
- [ICT security policy - information assurance strategy statement](#)

2.3 Privacy

Moj may require access to audit logs in investigating incidents (which may be of a purely technical nature such as a virus incident, but may also include investigations into malicious behaviour). Moj will comply with all relevant legislation in its monitoring and auditing activities. Moj provides you with computer equipment and systems to enable you to do your work. Moj will exercise its rights to ensure that its computer equipment and systems are used in a legitimate and lawful manner. This applies equally to providers.

More information about the Departments policy can be found here:

[HR - Conduct – IT usage guidance.](#)

3 ICT security infrastructure

In this section

- ICT security management
- ICT security responsibilities

3.1 ICT security management

The ICT security management structure falls within the overall departmental security management structure. The Permanent Secretary, as Accounting Officer, has overall responsibility for all aspects of security. The Departmental Security Officer (DSO) supports the Permanent Secretary by providing advice on personal and physical security policy and procedure. The IT Security Officer (ITSO) supports the DSO by providing advice on ICT security policy.

3.2 ICT security responsibilities

Senior Responsible Owner

The MoJ's Senior Information Risk Owner (SIRO) is responsible for the cross-Moj information risk policy and guidance and ensuring it continues to provide a suitable risk framework.

Moj Business Group/Area SIROs are responsible for implementing and managing information risk in their respective business groups and, reviewing the application of policy and guidance regularly thereafter to ensure it remains appropriate to their business objectives and risk environment.

Also, Moj Business Group/Area SIROs are responsible for authorising any exceptions and deviations from the ICT Security Policy.

3.2.1 Senior Responsible Owner

The Senior Responsible Owner (SRO) is the individual responsible and accountable for the successful outcome of the programme or project and achievement of the required business benefits.

3.2.2 Information Asset Owners

It is the responsibility of each project Senior Responsible Owner to ensure that the delivered information system meets the appropriate security standards. After the system has been implemented it is the responsibility of the Information

Asset Owner for that asset to ensure that all required technical, personnel, physical and procedural security controls are in place and adhered to.

3.2.3 ICT System Managers

It is the responsibility of the local ICT System Manager to ensure that all ICT security incidents are reported. The ICT System Manager is also responsible for providing ICT security advice to the system users based upon this ICT Security Policy, the ICT security guides and the user security documentation for the system. If in doubt ICT System Managers should contact their IT Service Desk for advice.

3.2.4 Managers' responsibilities

Managers are responsible for ensuring that all staff, including casuals and contractors:

- receive appropriate induction and training covering the use of Moj ICT equipment; are aware of the ICT Security Policy and adhere to it; have access to user guides for the computer systems and applications they use; have access to a copy of the *ICT Security Guide* and any other ICT security guides relevant to their work. (any consultants, contractors or agency staff that use their own computer equipment or equipment provided by their parent company must be made aware of and given access to the policy in the *Remote Working and Mobile Computing Security Guide*); and
- are provided with the resources needed for ICT security within their business area.

When a member of staff is known to be leaving, line managers have specific responsibilities. The manager is responsible for ensuring:

- the [Leaver's checklist](#), is completed and actioned;
- access to ICT-based systems is removed; and
- the appropriate handover of electronic data such as emails and MS Office files that may be required for business continuity – such data should be saved in an accessible location such as a shared drive so that information can be accessed when required

It is the responsibility of the manager and the member of staff who is leaving to make certain, before the last working day, that all records which require access and retention from email accounts, and any other electronic records, are moved to a storage area that is easily accessible. For areas of Moj that have access, this should be TRIM; for other areas a shared drive would be suitable. Accounts will not be permitted to remain open after staff have left Moj.

If the individual has left without notice, the leaving employee's activities will need to be undertaken by the line manager.

3.2.5 Individual responsibilities

You are responsible for all actions carried out on a computer under your 'user account' and for any computer equipment in your charge. You must:

- familiarise yourself with the ICT Security Policy and the contents of this guide;
- comply with the ICT Security Policy and the advice given in this guide;
- obtain further advice from your IT Service Desk if necessary;
- keep your computer user account passwords secret;
- protect all ICT equipment in your custody; and
- report all actual and suspected ICT security incidents through your ICT Service Desk (however your business area may have alternative arrangements for reporting misuse).

The **leaving employee** is responsible for:
working with the manager to follow the [Leaver's checklist](#), completing any tasks and returning any items requested in good time;

- ensuring the leaver's personal data is deleted; and
- placing an Out of Office Message on the account providing details of an appropriate alternative contact..

3.2.6 Moj ICT service providers

ICT service providers are responsible for ensuring that their staff and Sub-contractors adhere to Moj's ICT security policy, and that they deliver the security controls required for the systems they provide. More information can be found at [ICT Security Policy Framework](#).

4 Information Security

In this section

- Classification of Moj systems
- Passwords
- Access control
- Back-ups
- Information exchanges and data downloads
- Removable media
- Secure deletion and disposal
- Management of official records
- Possible pitfalls of MS Word

Introduction

This section is to assist the end users understanding of the security controls. There are specific technical policies that are available on request, please see [ICT Security Policy Framework](#)

4.1 Government Security Classification of Moj systems

Moj's ICT networks are secured to hold OFFICIAL information.

Only Moj computers may be connected to departmental networks. Any computer that is used to connect to the main departmental networks can be assumed to hold OFFICIAL information until it is securely deleted or disposed of.


4.2 Passwords

Access to most computer systems (referred to as 'log in' or 'log on') is controlled by a username and password. 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. Secure passwords are therefore crucial to the security of our computer systems. See Chapter 10 for more information on passwords.

Audit trail facilities can identify usage of Moj systems. You are responsible for what you do and may be held responsible for any actions carried out using your username and password. You must therefore not allow any one else to do work on any system using your ID and password.

4.3 Access control

If you leave your computer logged on when you are away from it, it may be possible for sensitive information held on the computer system to be used, read, changed, printed or copied by someone not authorised to see it. At the end of a working day, or if you are leaving your computer unattended for a long period of time during the day, log off from your computer and switch off the computer and screen. Do not touch the switches of any computer servers unless you are authorised to do so.

If you are leaving your computer unattended for a short period of time 'lock' your computer by activating your password protected screen saver or any similar 'locking' facility. A simple and quick way to lock your computer is to press  and L together. Use Ctrl, Alt and Delete to unlock it. If you are using a networked computer, always store your files, especially any sensitive or personal data, on the network drives rather than the local hard drive (usually called the C drive). Information held on network drives is protected much better than information held on the local hard drive. The local hard drive of a computer can be accessed by anyone who can log on to the computer, which will usually be all other users of the network, whereas access to network drives is controlled according to the access permissions granted to each network user.

4.4 Back-ups

ICT service providers regularly make copies of information stored on network and computer system servers and store these copies in a secure location. These copies or back-ups are made in order to help with the recovery of lost or corrupted information in the event of an error or ICT security incident. Backup copies are usually made overnight by ensuring that all of your data is stored on the network, e.g. on network drives or within an electronic document management system such as TRIM, you have the assurance that your files and documents are automatically backed-up. You may need to create local back-up copies, e.g. if your computer is not networked or if you manage a local server. Back-ups are valuable assets and should be protected in the same way as the movement of cash. You should regularly check that another computer can read information from the back-up copy. Local Business Managers should specific security guidance on wherever local back-ups are required.

4.5 Information exchanges and data downloads

If you need to move data the following link will explain that process and forms needed to do so securely [Moving Data](#).

4.6 Removable media

Removable storage media e.g. USB memory sticks, CDs, floppy disks and personal electronic devices, pose a significant threat to MoJ as it becomes much easier for data to be lost or stolen. In addition, connecting removable media that has not been provided by MoJ, or any authorised removable media that has been connected to non-Moj ICT systems, can pick up malicious software which could be dangerous to our networks and equipment. Removable media should not be used to store MoJ data. Only in exceptional circumstances, and where there is compelling business justification with no feasible alternative, will approval be given for the use of removable media.

Where removable media has been authorised it must be handled in accordance with the security classification system and protected as such, for example by using appropriate encryption; guidance will have been given at the time of approval.

Unencrypted removable media holding OFFICIAL information must not be removed from secure office premises without approval by a member of the Senior Civil Service and an approved business case.

USB memory sticks are of particular concern because they pose a greater threat than other types of removable media due to their physical size and storage capacity. Only USB memory sticks authorised and supplied by MoJ may be connected to MoJ ICT systems.

For information on laptops and personal electronic devices see Chapter 5 of the *Remote Working and Mobile Computing Security Guide*.

4.7 Secure deletion and disposal

All media should be securely disposed of. Electronic media that have been used to store OFFICIAL information must be securely deleted before being re-used or disposed of, or securely destroyed where re-use is not possible or required. The normal delete function available on the computer does not securely delete the data – special products and facilities must be used to meet HMG Standards. Contact your local Security Liaison Officer (SLO) or IA Lead for information on local deletion and disposal facilities for removable electronic media such as floppy disks, CDs, DVDs and USB memory sticks.

All computers, laptops and personal electronic devices, must be returned to the ICT service provider for re-use and disposal.

For re-use and disposal of any locally purchased ICT equipment, contact OperationalSecurityTeam@justice.gsi.gov.uk for advice.

5 ICT Security Incidents

In this section

- What is an ICT security incident?
- Reporting ICT security incidents

5.1 What is an ICT security incident?

An ICT security incident is any event that leads to, or may lead to, a breach of confidentiality, integrity or availability of information held on an ICT system.

Examples of ICT security incidents include:

- theft or loss of ICT equipment, software;
- theft or loss of data;
- malicious software (e.g. computer virus);
- wilful damage to computer or information held on it;
- unauthorised use of a computer;
- unauthorised amendment of information or software held on a computer;
- unauthorised disclosure of information;
- deliberate use of another person's password;
- misuse of software and hardware;
- use of unauthorised or unlicensed software;
- non-compliance with policies or guidelines;
- human errors (e.g. by programmers, system operators or system users);
- breaches of physical security arrangements;
- uncontrolled system changes;
- loss of service, equipment or facilities;
- system malfunctions or overloads; and
- malfunctions of software or hardware.

If you are in doubt as to whether a particular event constitutes a potential or actual ICT security breach, report it to your ICT Service Desk.

5.2 Reporting ICT security incidents

All actual or suspected ICT security incidents must be reported immediately. In general this will be to your ICT Service Desk, however your business area may have alternative arrangements for reporting misuse.

- If the actual or suspected incident involves loss of data, then the data access and compliance unit's reporting procedures must be followed (see [DACU Quick Guide](#)).
- ICT security incidents need to be recorded as soon as possible so that:
- their impact can be limited as soon as possible;
- remedial action can be taken to fix the problem;
- the effectiveness of current security measures can be assessed;
- we can learn from incidents;
- we can gain a better understanding of the risks to our information systems;
- we can prevent incidents happening again; and
- we can have confidence that our information systems are working correctly when no incidents are being reported.

Please see [IT Incident Management Policy](#) link for further information

6 Malicious software

In this section

- Malicious software
- Sources of malicious software
- Prevention of malicious software
- Responding to malicious software

6.1 Malicious software

Malicious software covers all software, which has been deliberately designed to harm computer systems, software and/or corrupt information. Malicious software takes several forms, categorised according to mode of transmission or execution. You may hear the terms Viruses, Trojan Horses, Logic Bombs and Worms to describe these different types.

6.2 Sources of malicious software

Malicious software can be distributed via:

- web sites;
- email; and
- removable media.

Malicious software is most commonly introduced onto a computer system by:

- an automatic download from an internet site (malicious code which is downloaded as soon as you visit the site);
- email attachments;
- unprotected or poorly protected connections to the Internet;
- any form of computer storage media supplied by maintenance engineers, contractors, visitors or colleagues;
- mobile code (e.g. ActiveX components);
- installing software, including freeware and shareware;
- computer storage media used to transfer data from home computers (e.g. infected USB sticks, CDs and DVDs); and
- commercial software.

6.3 Prevention of malicious software

To assist in prevention you must:

- only use Moj authorised software from approved sources;
- not copy software to give to other people;
- not load unauthorised software such as wallpaper, screen savers and games on to your computer;
- not use removable media unless you have an approved business case

6.4 Responding to malicious software

If your PC/laptop becomes infected, as notified by the anti-virus software on the computer, you should:

- stop using the computer (do not log off or switch it off) and put a note over the keyboard to ensure other people do not use it;
- report it to your ICT Service desk; and
- inform your line manager.

If your computer is operating in any other abnormal way, you should report it to your ICT Service Desk.

7. Electronic Messaging

In this section

- What is Electronic messaging
- Risks of using email
- Using email
- Government Secure Intranet (GSI)
- Criminal Justice Exchange (CJX)
- Criminal Justice Secure Email (CJSE)
- Additional measures for using secure email
- Using CJSE securely
- Email via Internet

What is Electronic Messaging

- Electronic messaging includes emails, instant messaging, messaging within social media sites (for example facebook and Twitter but there are many others) and mobile messaging such as SMS messages on BlackBerry or other MoJ issued telephones.

7.1 Risks of using electronic messaging

There are security risks inherent in using electronic messaging, some of which can be countered by technical measures which are the responsibility of our ICT service providers, but many of which are the responsibility of the electronic messaging user.

The risks you may run every time you send an electronic message include: unwittingly committing MoJ, or yourself, to a contractual relationship; sending material whose possession is contrary to UK law (e.g. 'obscene' material); expressing views which are contrary to UK law (e.g. inciting race hatred, or distributing defamatory material); breaching confidentiality by sending or forwarding OFFICIAL information across the internet or insecure electronic messaging system (see below); and breaching the Data Protection Act (e.g. by disclosing personal data to someone not entitled to see it).

You also need to be aware that unnecessary electronic messages or unnecessary communication to a large number of other people uses up valuable computer resources and your and other people's time.

7.2 Using electronic messaging

Moj does monitor the use of electronic messaging on Moj ICT systems and Moj provided devices. Your manager can request reports detailing your activity if they suspect misuse of a Moj ICT system that you use to send or receive electronic messages. The content of these reports will be considered by your manager and a nominated HR representative. More information can be found on the HR My Services page of the Moj Intranet within the [HR – Conduct – IT Usage Guidance](#).

You must:

- only use email in a way that is consistent with your duties or is sanctioned by your line manager. Reasonable personal use is allowed, provided that it is sanctioned by your line manager and it does not interfere with the performance of your duties and does not breach ICT security policy. You should be aware that your external email address identifies Moj, so is equivalent to using Moj letter-headed paper;
- remain polite and respectful of the feelings and beliefs of others when writing emails.

You must not:

- send emails or email attachments that contains obscene, profane, inflammatory, threatening, harassing (racially, sexually or otherwise), disruptive, or otherwise offensive language and including anything that will reflect poorly on Ministry of Justice's name or reputation;
- make any statements in emails or email attachments that may defame, slander or tend to lower the reputation of any person or organisation (or their goods or services) – you may be found personally liable for any defamatory statements, and Moj may also be liable for them;
- conduct trivial debates or exchanges with one individual or with a group of individuals;
- include unsuitable attachments such as video clips, images and executable files unless there is a genuine business reason to do so;
- send emails to large numbers of people unless absolutely necessary;
- send or forward unsolicited emails including jokes and chain letters;

All external mail should be automatically appended with a disclaimer notice so ordinarily no disclaimer notice needs to be added (if in doubt check with your ICT Service Desk). However, if you are exchanging email with an outside organisation with which Moj could be bound contractually the following text must also be appended:

"I am not authorised to bind the Ministry of Justice contractually, nor to make representations or other statements which may bind the Ministry of Justice in any way via electronic means."

If you are authorised to bind Ministry of Justice contractually via email you must indicate that you do have this authority plus the extent of and limitations to this authority;

- email sensitive information, such as protectively marked information across unsecured networks or to insecure email addresses (see below);
- not email sensitive information, such as information marked PERSONAL for an individual's attention, or other similar limited-distribution material, to a group or shared email address; or
- report the receipt of any email that breaches these email standards to your ICT Service Desk.

Also:

- you should avoid sending large attachments as these can have a detrimental affect on the computer network and there is no guarantee that the recipient is able to receive them;
- you should ensure that all external mail includes your name, your position/job title and your telephone number;
- you must not impersonate any other person when using email;
- if an email is being passed through several people for comment and amendment, it is important that the changes are highlighted and show who has made the change; and
- you should note that any personal financial transactions are carried out at your own risk and Ministry of Justice will not be held responsible for any losses you may incur.

7.3 Criminal Justice Exchange (CJX)

The Criminal Justice Exchange (CJX) is a secure data network designed to interconnect police forces in England, Scotland and Wales. CJX electronic messaging addresses are in the format: username@organisation.pnn.police.uk. GSi communities may exchange email up to OFFICIAL with CJX users.

7.4 Criminal Justice Secure Electronic messaging (CJSM)

Criminal Justice Secure Email (CJSM) provides a secure electronic messaging system between Criminal Justice Organisations and practitioners. A CJSM email address will have either of the two following formats:

username@organisation.co.uk.cjasm.net or **username@organisation.cjasm.net**.

GSI organisations may exchange OFFICIAL email with CJSM users.

7.5 Additional measures for secure electronic messaging

Where use of additional measures has been advised the sender needs to be sure:

- that the recipient has a need to know;
- that a risk management decision to release the information has been made by the appropriate responsible senior manager;
- that there is sufficient confidence/assurance that the recipient will give the OFFICIAL information the appropriate level of protection;
- that the following caveat is included in the document/electronic messaging:

"This document has been provided on a strictly 'Need-To-Know' basis.
For the storage and control of assets marked OFFICIAL you should do everything possible to:

- Make accidental compromise or damage unlikely during storage, handling, use, processing, transmission or transport.
- Deter deliberate compromise or opportunist attack.
- Dispose of or destroy in a manner to make reconstruction unlikely."

7.6 Using CJSJ securely

CJSJ is not a substitute for an approved remote working solution and must not be used as such by staff or contractors. It must only be used from: MoJ-provided computer equipment with adequate security measures in place such as approved hard disk encryption; computer equipment used by contractors/consultants as professional tools of their trade, with adequate security measures in place such as approved hard disk encryption.

CJSJ must not be used from public, personal, home or family computers.
CJSJ should only be used for legitimate business purposes relating to the Criminal Justice System.

8 Intranet, GSi and the Internet web sites

In this section

- Intranet and GSi web sites
- Internet world wide web

8.1 Intranet and GSi web sites

Moj intranet sites are private to Moj or to parts of Moj. The GSi hosts a number of GSi sites belonging to various government organisations and communities of interest (such as Librarians, IT Security Officers, Government Social Researchers and Government Legal Service) that are only accessible to GSi users. Browsing on these intranet web sites is safe but you should be aware that they include links to internet web sites (i.e on the world wide web or the web).

8.2 Internet world wide web

Moj monitors the use of web browsing and your activity will be logged. Under the IT Misuse procedure your manager can request reports detailing your activity if they suspect inappropriate use of web-browsing facilities. The content of these reports will be considered by your manager and a nominated HR representative and can lead to disciplinary action being taken.

- You should be aware that some sites might have malicious software such as damaging ActiveX controls, Java applets or JavaScript.
- Any data sent to and received from secure web sites, such as those using https (e.g online banking) may be momentarily decrypted, scanned for malicious content and then re-encrypted by our network.

9 Other Internet services

In this section

- Web-based email
- Internet-based instant messaging
- Bulletin boards and newsgroups
- Social networking
- File transfers
- Internet shopping
- Other Internet services

9.1 Web-based email

Email accessed via web-based email services bypasses anti-virus protection located on the GSi and Moj email servers so these services pose a significant risk to Moj's computer systems. For this reason you should not access web-based email unless you have an approved Business Case to do so.

9.2 Bulletin board and groups

If you subscribe to a bulletin board, newsgroup or discussion group (such as Yahoo or Google groups) you run the risk of disclosing your email address which may make you a target for spam (or junk/unsolicited) emails and email address spoofing.

9.3 Social networking

Social networking sites such as Facebook and MySpace pose security risks to Moj and to individuals. Sites like these are often used as a host for malicious software, which could try and attack Moj systems. Individuals could inadvertently release sensitive information about themselves, or about Moj.

Social networking sites often have functionality such as web mail and instant messaging, which can also lead to the introduction of malicious code and the unauthorised export of data.

- Do not disclose sensitive personal information about yourself or others.
- Do not disclose details about your job or which Department you work for.
- Do not make negative comments about Ministry of Justice.
- For further information about social media policy see;
[**Social Networking and Video Streaming.**](#)

9.4 File transfers

All For the latest and up to date guidance on secure transfer of data see
[**IT Security – Removable media.**](#)

10 Passwords

In this section

- Password policy
- Choosing a good password

10.1 Password policy

Access to most of MoJ's ICT systems is controlled by the use of user identifiers (user IDs) and passwords. Unless specifically authorised passwords must not be shared.

Office automation systems provide facilities for controlled file sharing and delegate access to mailboxes and calendars for colleagues, managers and personal assistants which make it unnecessary to allow anyone to use your network account. Make use of these facilities – **do not share your password**.

In order for a password to give an adequate level of security they must be correctly chosen, used and managed:

- your password should be of sufficient length and complexity to ensure it is difficult to guess or decrypt (passwords on MoJ ICT systems should be at least nine characters long);
- you should choose your password in a way that makes them difficult for other people to guess it;
- you should change your password at least once every three months or when prompted by the system;
- change your password if you think someone else may know it or if it has been disclosed to someone else;
- memorise your password, do not write it down, and if there is a genuine business reason for recording and storing a password it should be kept in a sealed envelope in a locked drawer or safe;
- do not use the same password for logins or sign-on to different systems; and
- do not re-use passwords (e.g. alternating the same two passwords).

10.2 Choosing a good password

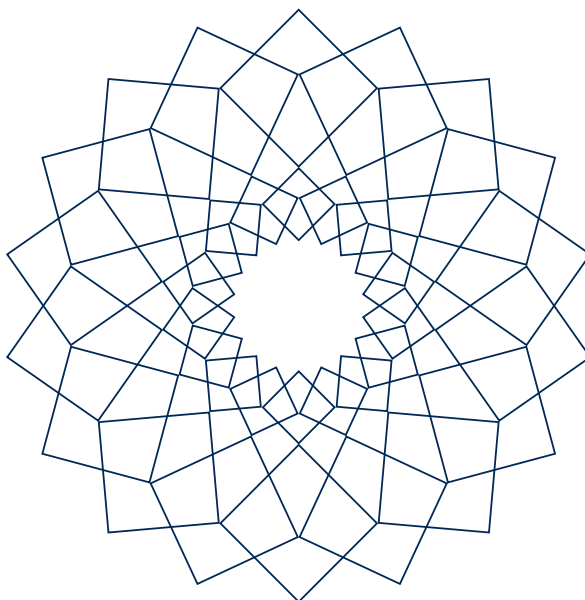
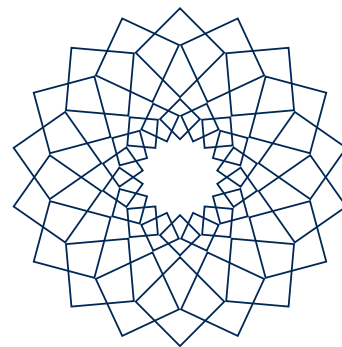
Choose passwords that are not easy to guess.

Use a mix of upper and lower case letters, numbers and symbols.

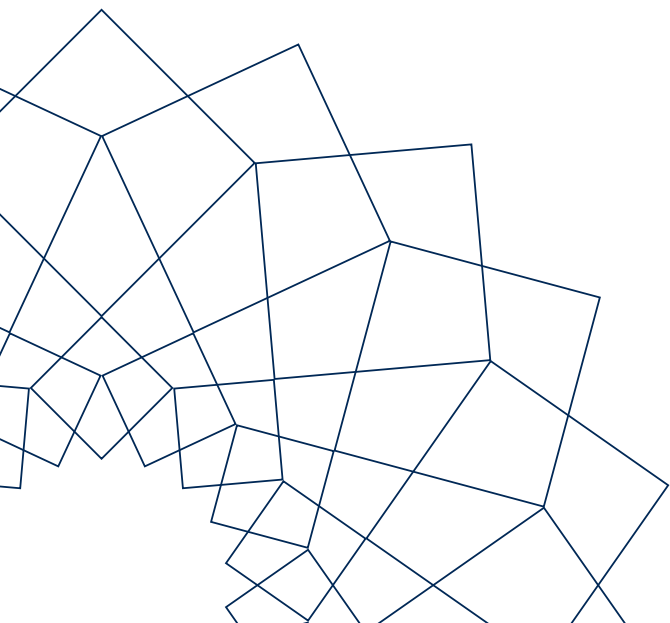
Do not use a recognisable word, though it can help with recall if the password is pronounceable.

Use the first letters of a phrase (e.g. 'This is now a Secure system for me!' would give a password of 'TinaSS4me!').

Do not make obvious letter / number substitutions to disguise recognisable words e.g. 0 for O, 5 for S, 1 for l, as this is a well known technique and therefore offers little security.



If you would like the information in this booklet in an alternative format, please email operationalsecurityteam@justice.gsi.gov.uk or ring 0161 234 2046.



**Produced by MoJ Technology IA
June 2014**