IT Acceptable Use Policy

# IT Acceptable Use Policy

This document is the Ministry of Justice (MoJ) ICT Security – IT Acceptable Use Policy. It provides the core set of ICT security principles and expectations on the acceptable use of MoJ ICT systems.

## Introduction

MoJ ICT systems and services are first and foremost provided to support the delivery of MoJ's business services. To achieve this, most MoJ users are provided with an appropriate general purpose computer environment (i.e. a standard MS Windows desktop) and access to services and communication tools such as e-mail and the Internet.

This policy outlines the acceptable use of MoJ IT systems and services, and, expectations the MoJ has on its staff in this area.

## Scope

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

Failure to adhere to this policy could result in:

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

POL.ITAUP.001

All Users **must be** made aware of the IT Acceptable Use Policy (this document) and provided with security awareness training which covers this policy.

POL.ITAUP.002

All Users **must undergo** refresher security awareness training which covers 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 MoJ ICT systems. All Users have a role in protecting the information assets which are under their control or have access to.

MoJ ICT 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 know as Security Operating Procedures (SyOPs).

It is important that all Users of an ICT system (include support and system administrative Users) are familiar with these SyOPs and are provided with the appropriate training.

POL.ITAUP.003

All ICT systems **must have and maintain** a set of Security Operating Procedures (SyOPs). For systems undergoing the Accreditation process, these SyOPs can be included as part of the RMADS.

POL.ITAUP.004

All Users of an ICT system (this includes support and system administrative staff) must read the SyOPs applicable and **must acknowledge** that they have both read and understood it before being granted access. A record must be kept of this event and made available to the system Accreditor upon request.

POL.ITAUP.005

All Users **must be** made aware that non-conformance to system SyOPs constitutes a breach of the MoJ IT Security Policy which may result in disciplinary action.

POL.ITAUP.006

Any change to an ICT system's SyOPs **must be** approved by the system Accreditor in advance.

POL.ITAUP.007

Any request to perform an action on an ICT system which contravenes its SyOPs **must be** approved by the system Accreditor or MoJ ITSO in advance.

For most Users, access to MoJ ICT systems and information held on them is through using a desktop terminal, remote access laptop and/or mobile device (such as a Blackberry 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 [ICT Security - Information Classification and Handling Policy](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/information-classification-and-handling-policy/).

### General Security Operating Procedures (SyOPs)

The policy refers to a key set of general SyOPs which are listed below:

* [IT Security Operating Procedures - System Administrators](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/system-administrators/).
* [IT Security Operating Procedures - Administrators and Users](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/system-users-and-application-administrators/).
* [Remote Working](remote-working.html).
* IT Security Operating Procedures - ICT Equipment: Desktop – Corporate.
* IT Security Operating Procedures - ICT Equipment: Mobile Devices - RAS Laptop.
* IT Security Operating Procedures - ICT Equipment: Mobile Devices – Blackberry.

To minimise the number of SyOPs in circulation and standardise procedures, the SyOPs listed above act as the primary set where individual ICT systems are expected to conform to in terms of their own SyOPs. Any deviations or additions are at the discretion of the system Accreditor.

POL.ITAUP.008

All ICT systems **must have** documented SyOPs which comply with the general SyOPs listed in this policy (see [here](#Xb7c38db1f23c16d258404ac28f176a027eb40ec) ). Any deviations or additions must be recorded in separate SyOPs which form an addendum to one of the SyOPs listed [here](#Xb7c38db1f23c16d258404ac28f176a027eb40ec).

**Note** – An ICT system may make use of, in their entirety, one or more of the SyOPs listed above as the procedures of that IT system do not deviate from those described in these general SyOPs.

### Removable Media

Removable storage media include devices such as USB memory sticks, writeable CDs/DVDs, floppy discs and external hard drives. These devices can potential contain large amounts of protectively marked data and pose a significant risk to the Confidentiality of data held on them. As such, the MoJ controls the use of removable media through SyOPs, technical security controls, and requiring movements of bulk data to be authorised by MoJ ICT IA, this includes completing an Information Asset Movement Form.

POL.ITAUP.009

Any removable media device **must be** approved by MoJ ICT IA where that device is used to store protectively marked data. The type of device and associated SyOPs must be approved by the system Accreditor prior to operational use.

POL.ITAUP.010

All Users **must ensure** that all data stored on or transported by removable media is in accordance with the applicable system SyOPs.

POL.ITAUP.011

All Users **must seek** approval from MoJ OST prior to any bulk transfer of protectively marked data using removable media. MoJ ICT IA will advise on any technical and procedural requirements such as data encryption and handling arrangements.

### Passwords

The username and password combination, in the main, is the primary access credential used for authenticating a User to an ICT systems and authorising their 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 **must not** share or disclose any passwords with any other person.

POL.ITAUP.013

All Users **must not:**

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

## Legal and regulatory requirements

There are a number of legal and regulatory requirements for which the MoJ must comply with, this in addition to HMG security policy as expressed in the [HMG Security Policy Framework](https://www.gov.uk/government/publications/security-policy-framework).

POL.ITAUP.014

All Users **must be** made aware of legal and regulatory requirements they must adhere to when accessing MoJ ICT systems. This must be included as part of the SyOPs.

## MoJ's Corporate Image

Communications sent from MoJ ICT systems or products developed using them (e.g. MoJ branded document or PowerPoint presentation) can damage the public image of the MoJ if, it is for purposes not in the interest of the MoJ, or, it is abusive, offensive, defamatory, obscene, or indecent, or, of such a nature as to bring the MoJ or any its employees into disrepute.

POL.ITAUP.015

All Users **must ensure** that MoJ ICT systems are not used in an abusive, offensive, defamatory, obscene, or indecent, or, of such a nature as to bring the MoJ or any its employees into disrepute.

## Potential to cause offence and harm

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

POL.ITAUP.016

MoJ ICT systems **must not** be used for any activity that will cause offence to MoJ employees, customers, suppliers, partners or visitors, or in a way that violates the [MoJ Code of Conduct](https://intranet.justice.gov.uk/guidance/hr/conduct-behaviour/).

## Personal use

The MoJ permits limited personal use of its ICT systems provided this does not conflict or interfere with normal business activities. The MoJ monitors the use of its IT systems and any personal use is subject to monitoring and auditing (see [here](#monitoring-of-communications) ), and may also be retained in backup format even after deletion from live systems.

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

* Filtering of Internet and e-mail traffic – All Internet and e-mail traffic is filtered and analysed, further details are provided [here](#X1c339fc6bb37a87e2af818c081b07bfc644a0f8).
* Policy and procedures – This policy and associated SyOPs set out the restrictions placed on the use of an ICT system.

POL.ITAUP.017

Users **must ensure** any personal use of MoJ ICT systems does not conflict or interfere with normal business activities. Any conflict is to be reported to their line manager.

POL.ITAUP.018

Users **must ensure** that any personal use of MoJ ICT systems is inline with any applicable SyOPs and this policy.

POL.ITAUP.019

Users **must be** aware that any personal use of MoJ ICT systems which contravenes any applicable SyOPs, or this policy, constitutes a breach of the IT Security Policy and may result in disciplinary action.

## Maintaining system and data integrity

Users need to 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 will affect either the integrity of that system or the integrity of shared data needs to be undertaken or supervised by authorised User or system Administrator.

POL.ITAUP.020

All Users **must request** any changes to ICT system/s or ICT equipment through the IT helpdesk. Further details are provided in [IT Security Operating Procedures - Administrators and Users](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/system-users-and-application-administrators/).

## Electronic messaging and use of the Internet

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

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

Also, the use of any high bandwidth services, such as video steaming websites, creates network capacity issues which cause the poor performance key MoJ ICT services. As such, the MoJ restricts access to the Internet based on job role. Amendments can be made on the submissions of a business case for approval by MoJ Operational Security Team (OST).

The MoJ will regard as a disciplinary offence any usage of electric communications (e-mail and other methods such as instant messaging) and the Internet which, breaks the law, contravenes MoJ HR policies, or involves unauthorised access or handling of material that is deemed to be inappropriate, abusive, offensive, defamatory, obscene or indecent.

External E-mail 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 MoJ deploys a number of security controls to protect its Users from Internet and e-mail borne attacks, however these controls are reliant on Users to remain vigilant, follow any applicable SyOPs, and report any suspicious behaviour.

POL.ITAUP.021

All Users **must use** the Internet and e-mail (and other electronic communication systems) in accordance with this policy document.

### Managing e-mail use

Users are responsible for ensuring that all information is handled in line with protective marking of that information in accordance with [IT Security - Information Classification and Handling Policy](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/information-classification-and-handling-policy/).

The MoJ is connected to the Government Secure Intranet (GSi), which provides a secure environment for sending/receiving E-mails between Government departments. This allows Users with a MoJ E-mail account (e.g. suffix '@justice.gsi.gov.uk') to send E-mails which attracts a protective marking up to and including RESTRICTED to another MoJ or government User where their E-mail suffix ends in '.gsi.gov.uk'.

POL.ITAUP.022

All Users **must ensure** that protectively marked information contained within or attached to an e-mail is handled in accordance with [ICT Security - Information Classification and Handling Policy](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/information-classification-and-handling-policy/).

E-mail is a major source of malware and route into the MoJ for criminal organisations to defraud staff or exfiltrate information. All Users need to exercise care when handling emails and report any suspicious activity as an IT security incident.

POL.ITAUP.023

All Users **must ensure** that they do not:

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

POL.ITAUP.024

Where a User suspects that an E-mail received is from an untrusted, unknown or unsolicited source, they **must** report it as an IT security incident.

## Connectivity and remote access

Remote access is provided to MoJ ICT systems and services allowing Users access from offsite and home locations to connect in. The main methods of access are either via a RAS laptop and/or Blackberry device. In the main, remote access is to a protectively marked MoJ IT system (up to and including RESTRICTED). As such Users need to be aware of both the security controls and procedures of the device used as well as the general physical security considerations. This includes any restriction on the carriage of such devices as they may contain HMG protectively marked data and HMG cryptographic material.

MoJ ICT IA maintains a list of countries where carriage and use of remote access devices is permitted. Further details can be found in the [Remote Working](remote-working.html) guidance.

POL.ITAUP.025

All Users **must be** aware of the [Remote Working](remote-working.html) guidance and must confirm that they have read and understood it before being provision with any remote access devices or equipment (e.g. RSA token).

POL.ITAUP.026

Any User wishing to take a remote access device out of the UK **must consult** [Remote Working](remote-working.html) before doing so or the applicable device IT Security Operating Procedures document.

## Monitoring of communications

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.

The MoJ monitors telephone usage, network, email and Internet traffic data (including sender, receiver, subject; attachments to an e-mail; 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.

The MoJ, so far as possible and appropriate, respects the privacy and autonomy whilst working of all Users, but further to [this information](#personal-use), any personal use of MoJ ICT systems will also be subject to monitoring. By carrying out personal activities using MoJ ICT systems, Users are consenting to the MoJ processing any sensitive personal data which may be revealed by such monitoring (for example regular visits to a set of websites).

For the purposes of business continuity it may sometimes be necessary for the MoJ to access business communications (including within e-mail mailboxes) while a User is absent from work (including holiday and illness). Access will only be granted through submission of a formal request to the IT Helpdesk where approval is required from the relevant line manager where the MoJ ITSO and MoJ HR may be consulted.

POL.ITAUP.027

All Users **must be** aware their electronic communications are being monitored in accordance with this policy.

POL.ITAUP.028

All Users **must be** aware that business communication (such as e-mail mailboxes) may be accessed if they are absent from work. This can only be requested and authorised by a line manager where the MoJ ITSO and MoJ HR may be consulted.