Data Handling and Information Sharing Guide

# Data Handling and Information Sharing Guide

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

## Overview

### Introduction

The [Government Functional Standard - GovS 007: Security](https://www.gov.uk/government/publications/government-functional-standard-govs-007-security) identifies mandatory requirements about the value and classification of information assets. To comply with these requirements, the MoJ needs to ensure that:

Where information is shared for business purposes, departments and agencies must 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 must 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](information-classification-and-handling-policy.html), whilst this document sets out the MoJ guidance sharing information within the MoJ 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 OFFICIAL with the SENSITIVE handling caveat, often written as OFFICIAL-SENSITIVE. While this approximate correspondance might be helpful, you should always review classification where older terms are used, to ensure that the correct current classification is used.

### Scope

The MoJ Information Assurance (IA) team provide general guidance on the handling of protectively marked data, whilst this document concentrates on providing guidance on information stored on MoJ IT systems and exchanged electronically within the MoJ and with external parties.

This guide is split into three sections:

* Handling data on MoJ IT systems.
* Information sharing.
* Reporting data loss.

A [Data Movement Form](#data-movement-form-dmf) must be completed for all transfers where information is transferred from an MoJ IT system to another MoJ IT system or external party. Further details on the form can be found [here](#data-movement-form-dmf).

Note: This document provides guidance for handling and sharing of information and data up to and including OFFICIAL and OFFICIAL-SENSITIVE, or the older Impact Level (IL) 3. Where information attracts a high protective marking or IL, advice must be sought from the MoJ Operation Security Team (OST) and MoJ IT Security Officer (ITSO).

### Demonstration of Compliance

The [CESG Information Assurance Maturity Model (IAMM)](https://www.ncsc.gov.uk/guidance/information-assurance-maturity-model-and-assessment-framework-gpg-40) sets out the minimum maturity level Government departments should attain. Safeguarding data is captured as a basic requirement in Level 1 and the MoJ will need to demonstrate compliance against this requirement.

## Handling data on MoJ IT systems

This section covers how data must be handled on MoJ 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 SENSITIVE. See the [Information Classification and Handling Policy](information-classification-and-handling-policy.html) for further details.

### Ownership of information

All MoJ 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 must 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 must 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 MoJ 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](#usb-mass-storage-device).

##### Secure network (system-to-system electronic transfer)

The MoJ preference for transferring data is to use a secure accredited government network whether that is a MoJ 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 OFFICIAL-SENSITIVE, 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. See the [Access Control Guide](access-control-guide.html) for further information.

Any additional controls must be captured on the DMF (see [Data Movement Form](#data-movement-form-dmf) where advice should be obtained from the MoJ Chief Information Security Office (CISO) 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, see the [Removable Media](removable-media.html) guidance.

The type of device selected is normally dependant on the sensitivity of the data and the amount of data being transferred. Advice must be sought from the Operational Security Team: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk), or CISO on the best option to use when completing the DMF (see [Data Movement Form](#data-movement-form-dmf)).

##### Optical media

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

#### Data at rest on MoJ-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. MoJ-issued laptops use an approved whole disk encryption product. This allows data to be safely stored.

#### Disposal and decommissioning

Sensitive data must not be kept for longer than is needed. The IAO must check for compliance, including any mandatory retention period.

Physical media containing sensitive data must 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](secure-disposal-of-it-equipment.html) guidance.

## Information sharing

### General principles

Where there is a business need to transfer sensitive data, it must 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 must ensure that any data shared can be adequately secured by the recipient. The sensitivity of data must 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

MoJ staff, including contractors and agency staff, must 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 MoJ staff must avoid exposing sensitive data to unnecessary risks, in particular by observing all aspects of the MoJ [Acceptable Use Policy](acceptable-use-policy.html).

Authorisation must 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](#data-movement-form-dmf). the following sub-sections provide guidance on particular types of information sharing common across the MoJ, and to help you complete a DMF.

#### Internally within the MoJ

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

Where information is transferred between MoJ 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 MoJ IT systems requires a completed and authorised [Data Movement Form](#data-movement-form-dmf) using one of the [data in transit](#data-in-transit) options.

#### Information sharing with other HMG department

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

#### Information sharing with external 3rd parties

Any transfer of sensitive data to a 3rd party, including sub-contractors or service providers, must be authorised by the relevant IAO. An appropriate contract, [Data Movement Form](#data-movement-form-dmf), and Non-disclosure Agreement (NDA) must be in place prior to the transfer. It might also be appropriate to establish a [Security Aspects Letter (SAL)](security-aspect-letters.html) and Codes of Connection (CoCo) agreement.

Where the information is OFFICIAL-SENSITIVE, it must 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](#data-in-transit) options.

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

##### Sharing across an unsecured network

Sensitive data must 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](#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 e-mail.

#### Sharing information above OFFICIAL

Where there is a business requirement to share information classified higher than OFFICIAL, advice must be sought from the Operational Security Team: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk) or CISO prior to completing a [Data Movement Form](#data-movement-form-dmf).

## Data Movement Form (DMF)

The purpose of the DMF is to ensure that the movement of information assets is secure, and in compliance with the [Government Functional Standard - GovS 007: Security](https://www.gov.uk/government/publications/government-functional-standard-govs-007-security)

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

## Using SecureZIP

SecureZip is a compression and encryption product which can be used to encrypt sensitive data for use in removable media and e-mail 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 e-mail 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.

### Best practices for everyone

The MoJ password guidance follows [NCSC guidance](https://www.ncsc.gov.uk/guidance/using-passwords-protect-your-data). The NCSC recommends a [simpler](https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach) 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](https://www.cyberaware.gov.uk/passwords) 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.

If a system or another person provides you with a password, change it before doing any MoJ 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 must 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 must 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 |

## General enquiries, including theft and loss

**Dom1/Quantum - Technology Service Desk**

* Tel: 0800 917 5148

Note: The previous itservicedesk@justice.gov.uk email address is no longer being monitored.

**Digital & Technology - Digital Service Desk**

* Email: [servicedesk@digital.justice.gov.uk](mailto:servicedesk@digital.justice.gov.uk)
* Slack: #digitalservicedesk

**HMPPS Information & security:**

* Email: [informationmgmtsecurity@justice.gov.uk](mailto:informationmgmtsecurity@justice.gov.uk)
* Tel: 0203 334 0324