#Secure Data Transfer Guide

##Introduction

This guide outlines the security procedures and advice for Ministry of Justice (MoJ) staff wanting to send or receive data securely from external sources.

This is important to the MoJ, because personal and sensitive data is regularly transmitted between departments. Legislation such as GDPR, and industry standards such as PCI DSS, affect the MoJ’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 MoJ works to protect.

##Who is this for?

This policy is aimed at three audiences:

1. **Technical users**: these are in-house MoJ 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 MoJ 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 MoJ.
3. **General users**: all other staff working for the MoJ.

The phrase “all MoJ 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 MoJ, 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 MoJ?
* 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 **SHALL**:

* 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 MoJ is the controller of the data being transferred, the security storage requirements at the destination **SHALL** 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 [Data Privacy Team](mailto:privacy@justice.gov.uk) 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 **SHALL** be informed, to decide if a Data Protection Impact Assessment is required.

##Data Transfer

Normally, files **SHOULD NOT** be transferred by email. Normally, files **SHOULD** 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 MoJ’s preferred method of data sharing is to use Microsoft Teams via Sharepoint. Teams has been authorised to hold OFFICIAL-SENSITIVE information. It is configured to provide greater granular protection through tools such as Azure Information Protection (AIP). Where possible, data **SHOULD** be transferred using Teams.

Due to the diverse nature of the MoJ’s architecture, using Teams might not always be possible. Those in the MoJ Digital and Technology team who do not have access to Microsoft Teams **MAY** use Google Workspace to transfer data.

For more details on the actual process for a transfer, contact the [Cyber Assistance Team](mailto:CyberConsultancy@digital.justice.gov.uk).

##Data Transfer by email

Where it is not possible to use Microsoft Teams or Google Workspace, **AND** the data to be transferred is less than 20MB, email **CAN** be used, **BUT** the following requirements **SHALL** be met:

* Email communication **SHOULD NOT** be used to transfer unencrypted sensitive or personal data. Employees **SHOULD** note that emails are not designed to attach and transfer large amounts of data. The MoJ’s email system does not support file attachments that exceed a total of 20MB.
* You **SHOULD** 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 **SHALL** 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 **SHALL** contain clear instructions of the recipient’s responsibilities, and instructions on what to do if they are not the correct recipient.
* Information sent **SHALL**, where practical, be enclosed in an encrypted attachment.
* Care **SHALL** be taken as to what information is placed in the subject line of the email, or in the accompanying message. Filenames or subject lines **SHALL NOT** reveal the contents of attachments. Filenames or subject lines **SHALL NOT** disclose any sensitive personal data.
* Emails **SHALL** only be sent from your work email address, as provided by the MoJ. 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 **SHALL** only be used for purposes relating to the criminal justice service.

##Microsoft 365 Encrypted email

* This facility is available for standard individual and generic MoJ email accounts
* This method **CAN** be used to send or receive files classified as OFFICIAL. It is normally used with external partners, agencies, or individuals who cannot be contacted using CJSM email.
* The attached files on a single email **CAN NOT** exceed 25MB.

##Removable storage devices

The MoJ 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 **MAY** be used with caution.

Any data being transferred by removable media such as a USB memory stick **SHALL** be encrypted. Encrypted portable storage devices **SHALL** be password protected with a strong password. All passwords **SHALL** 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 [Operational Security Team](mailto:OperationalSecurityTeam@justice.gov.uk).

Ownership of any removable media used **SHALL** be established. The removable media **SHALL** be returned to the owner on completion of the transfer. The transferred data **SHALL** 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, **SHALL** accompany the removable media.

Any accompanying message or filename **SHALL NOT** reveal the contents of the encrypted file. The sender **SHALL** 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 [Operational Security Team](mailto:OperationalSecurityTeam@justice.gov.uk) immediately.

##Data transfers by post or courier

Data transfers using physical media such as memory cards or USB devices **SHALL** only be sent using secure post. Royal Mail First or Second class **SHALL NOT** be used. Royal Mail Special Delivery or Recorded Delivery **CAN** be used. For non-Royal Mail services, a secure courier service **SHALL** be used, with a signature obtained upon delivery. The recipient **SHALL** be clearly stated on the parcel. The physical media **SHALL** be securely packaged so that it is not damaged in transit.

The recipient **SHOULD** be told in advance that the data is being sent, so that they know when to expect the data. The recipient **SHALL** 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 **MAY** be used where removable media is used. When arranging for an individual to collect information, the identity of the individual **SHALL** be established, to confirm who they claim to be. An appropriate form of identification **SHALL** 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 **SHALL** be kept to a minimum.
* Personal or Confidential information **SHALL NOT** 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 **SHOULD** 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 **SHOULD** 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) **SHALL** implement strict certificate checking to maintain trust in end-points.

##Incidents and contact details

**Note:** If you work for an agency or ALB, refer to your local incident reporting guidance.

For help with incidents, including theft and loss, contact:

* **DOM1/Quantum - Technology Service Desk**
* Tel: 0800 917 5148
* **Note:** The previous itservicedesk@justice.gov.uk email address is no longer being monitored.
* **Digital and Technology - Digital Service Desk**
  + Email: [servicedesk@digital.justice.gov.uk](mailto:servicedesk@digital.justice.gov.uk)
  + Slack: #digitalservicedesk
* **HMPPS Information and security**
  + Email: [informationmgmtsecurity@justice.gov.uk](mailto:informationmgmtsecurity@justice.gov.uk)
  + Tel: 0203 334 0324

For non-technology incidents, contact the MoJ Group Security Team: [mojgroupsecurity@justice.gov.uk](mailto:mojgroupsecurity@justice.gov.uk)

Contact the Privacy Team for information on Data Protection Impact Assessments: [privacy@justice.gov.uk](mailto:privacy@justice.gov.uk)

If you are not sure who to contact, ask the Operational Security Team:

* Email: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk)
* Slack: #security

For any further questions relating to security, contact: [security@justice.gov.uk](mailto:security@justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).