Remote Working

# Remote Working

## Key points

* Be professional, and help keep Ministry of Justice (MoJ) information and resources safe and secure at all times.
* Think about where you are working, for example - can other people or family see what you are working on? Be thoughtful about information privacy.
* Never send work material to personal email accounts.
* Keep MoJ 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.
* Do not leave MoJ equipment unattended.
* Get in touch quickly to report problems or security questions.

## 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 MoJ, 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 MoJ, 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 MoJ mobile computing equipment.

## What is remote working?

Remote working means you are working away from the office. This could be from home, at another MoJ 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-MoJ 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.

**Always:**

* Keep MoJ equipment and information safe and secure.
* Protect MoJ 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.
* Keep your workspace clear and tidy - follow a 'clean desk policy', including paperwork, to ensure MoJ information isn't seen by unauthorised people.
* Use MoJ 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.

**Never:**

* Let family or other unauthorised people use MoJ equipment.
* Leave equipment unattended.
* Work on sensitive information in public spaces, or where your equipment can be overlooked by others.
* Advertise the fact that you work with MoJ materials.
* Take part in conference or video calls when you are in public or shared spaces such as cafes or waiting rooms.
* Send work material to your personal email address.

## Working securely

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

* **Work locations** - as with home working above, 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 eg conference and video calls.
* Keep MoJ **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 MoJ systems you access and work with.

## Using your own equipment

The main guidance is available [here](personal-devices.html).

Wherever possible, you should always use official MoJ equipment for business purposes. Never send work material to your personal email accounts.

If you are working remotely, or do not have access to MoJ equipment, it might be tempting to use your own equipment, especially printers. The advice is to avoid printing anything, and in particular not to use personal printers.

However, if you really must print MoJ information, you:

* should connect directly to the printer using USB, not WiFi
* should not print out personal information relating to others
* should consult the information asset owner or line manager before printing the information
* must store any and all printed materials safely and securely until you return to MoJ premises, when they must be disposed of or filed appropriately
* **must never** dispose of MoJ information in your home rubbish or recycling

Basically, think before you print.

## Privacy

It is important to protect privacy: yours and that of the MoJ. 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 MoJ 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 MoJ information. If anyone might see 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 see the information you are working with.
* Don't 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.

### 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

### Incidents

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

**Operational Security Team**

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

### Privacy Advice

**Privacy Team**

* Email: [privacy@justice.gov.uk](mailto:privacy@justice.gov.uk)
* Slack: #securityprivacyteam
* Intranet: <https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/>

### Cyber Security Advice

**Cyber Consultants & Risk Advisors**

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

### Historic paper files urgently required by ministers, courts, or Public Inquiries

**MoJ HQ staff**

* Email: [Records\_Retention\_@justice.gov.uk](mailto:Records_Retention_@justice.gov.uk)

**HMCTS and HMPPS staff**

* Email: [BranstonRegistryRequests2@justice.gov.uk](mailto:BranstonRegistryRequests2@justice.gov.uk)

### JustStore

* Email: [KIM@justice.gov.uk](mailto:KIM@justice.gov.uk)

## Related information

[NCSC Home working: preparing your organisation and staff](https://www.ncsc.gov.uk/guidance/home-working) [CPNI Home Working Advice](https://www.cpni.gov.uk/advice-home-working-0)

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

[HMPPS Advice](https://intranet.noms.gsi.gov.uk/support/information-policy-and-assurance/information-assurance)

Last updated: April 24th, 2020.