#User access

Acceptable use of Information Technology at work.

This guidance applies to all staff and contractors who work for MoJ.

Everyone working at the MoJ has access to MoJ Information Technology (IT) resources. You must use them in an acceptable way. This guidance explains what that means.

##Summary

Be sensible when using MoJ IT resources:

* The resources are for you to do MoJ work.
* Protect the resources at all times, to help prevent unacceptable use.
* If the use would cause problems, upset, offence, or embarrassment, it’s probably not acceptable.
* Context is important. Security risks can increase when working outside your normal workplace.
* Be aware that your use of resources is monitored. During an investigation into a security incident, IT forensic techniques capture evidence.
* If you’re not sure if something is acceptable, ask for help first.
* Above all, if you think there is a problem, [report it](/guidance/security/report-a-security-incident/) or ask for help.

The way you use IT is important, because it indicates your approach to work, and can be taken into account when assessing your behaviour and performance.

##What is meant by IT?

IT means the devices or services you use for creating, storing, or sharing information. This includes everything from devices (such as laptops, ’phones, mobile Wi-Fi hotspots (MiFi), iPads, tablets, printers, USB memory sticks) through to online services (citizen-facing online services, staff tools, corporate email).

##Acceptable use of MoJ IT

Acceptable use of IT is when you use it to do your work.

IT helps you complete your tasks as efficiently and effectively as possible. Sometimes, you might need account details such as passwords to use the IT. Acceptable use means protecting this kind of information, too.

Acceptable use can also vary according to context. For example, checking sensitive personal details might be perfectly normal within a secured office, but is not acceptable in a public space where anyone else might see those details.

##Unacceptable use of MoJ IT

Unacceptable use of IT prevents you or your colleagues from doing work, or is unlawful or illegal, or does not take the context into account.

There are many unacceptable uses of IT, making it impossible to provide a complete list. Examples of things to avoid include:

* Deliberately or accidentally sharing resources or information, such as passwords, with people who are not supposed to have them.
* Using resources without permission.
* Storing sensitive information where it could easily be lost or stolen.
* Using unapproved tools or processes to store sensitive information, such as passwords or credit card details.
* Using your work email address for personal tasks.
* Using a personal account or personal email address for work tasks.
* Excessive private use during working time.
* Installing unlicensed or unauthorised software.

##Why unacceptable use is a problem

Unacceptable use of IT might affect the MoJ in several ways, such as:

* Bad publicity or embarrassment.
* Increased or unexpected costs or delays.
* Civil or legal action.
* Reduced efficiency and effectiveness.

Unacceptable use might also affect you, too:

* Suspension of access, so that you cannot do your work.
* Disciplinary proceedings, up to and including dismissal.
* Termination of contract for contractors and agency staff.

##Keeping control

You are responsible for protecting your MoJ IT resources. This includes keeping your usernames and passwords safe and secure.

It also means looking after MoJ equipment, especially when working away from MoJ locations. You are responsible for protecting MoJ equipment issued to you. Any theft of MoJ equipment, or deliberate or willful damage to MoJ equipment, should normally be [reported](lost-devices-incidents.md) to the Police and to the Service Desk.

**Note:** You should normally report instances of theft or damage to authorities as indicated. However, there might be additional circumstances which mean a sensitive handling of the situation is appropriate. It is acceptable to consider the context of the situation when making a report. Ensure you can justify your actions. In cases of uncertainty, don’t hesitate to ask your line manager, or other responsible authority for advice.

While you might be careful about acceptable use of MoJ IT, there are still risks from [malware](https://en.wikipedia.org/wiki/Malware), [ransomware](https://en.wikipedia.org/wiki/Ransomware), or [phishing](https://en.wikipedia.org/wiki/Phishing) attacks.

If you get an email from anyone or anywhere that you are not sure about, remember:

* Don’t open any attachments.
* Don’t click on any links in the email.

If there is any doubt, or you are worried that the [email might be malicious](/news/ntk-phishing-dont-take-the-bait/) or inappropriate, [report it immediately](/guidance/security/report-a-security-incident/) as an IT security incident.

##Personal use of MoJ IT

Limited personal use of MoJ IT is acceptable as long as it does not cause a problem with your work or that of your colleagues. Context is important. For example, doing personal internet banking during your lunch break might be acceptable, but doing the same thing during a work meeting would not.

##Personal use of MoJ mobile phones

You might be allocated a mobile phone for use as part of your work. The mobile phone enables you to:

* Make or receive calls.
* Send or receive SMS texts.
* Use Internet services.

This usage must always be for work purposes.

Examples of unacceptable MoJ mobile phone use include:

* Making charitable donations from the mobile phone account.
* Signing up for premium rate text services.
* Calling premium rate telephone services.
* Voting in reality TV popularity contests - these usually involve premium rate services.
* Downloading, uploading, or streaming media files that are not work-related, such as music or movies.
* Tethering another device to the MoJ mobile phone, and then using the other device for any of the above activities.

… as well as any other activities that are not obviously work-related.

All use of MoJ IT resources is monitored and logged. This includes mobile phone usage listed in account bills. It is possible to see if you used a work-issued mobile phone for unacceptable activities. Unacceptable use is reported to your Line Manager for further appropriate action. Assessing your behaviour and performance takes this kind of activity into account.

##Using MoJ IT outside your usual workplace

Some IT resources might be usable [away from your usual workplace](/documents/2017/12/remote-working-and-mobile-computing-security-guide-november-2017.pdf), such as a laptop. Even outside the office, you must continue to ensure acceptable use of the IT resources.

You should also [ask](/guidance/security/it-computer-security/accessing-moj-it-systems-from-overseas/) before taking MoJ IT equipment outside the UK.

##Avoid using removable media

Removable media like memory sticks are portable and easy-to-use. Unfortunately, this makes them a security risk, so [avoid using them](/guidance/security/it-computer-security/removable-media/). If however they are essential to your work, follow the [Use of Removable Media](/guidance/security/it-computer-security/removable-media/) guidance.

##Personalisation of equipment

A popular trend is to adorn laptops with stickers. This is acceptable as long as the material does not cause problems such as upset, offence, or embarrassment. The same applies if you customise the desktop environment of your equipment, for example by changing the desktop image.

##Contacts

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](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).