Acceptable use of information technology at work

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

Summary

2. Be sensible when using MHCLG IT resources:

- the resources are for you to do MHCLG work
- protect the resources at all times to help prevent unacceptable use
- If you think the use would cause problems, upset or embarrassment, then it's probably not acceptable
- context is important: remember that security risks can increase when working outside your normal workplace
- be aware that your use of resources is monitored and that as part of an investigation into a security incident, IT forensic techniques might be used to capture evidence. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.
- if you have any doubt about whether something is acceptable, ask for clarification or permission first
- above all, if you think there is a problem, report it or ask for help

What is meant by IT?

3. IT means the devices or services you use for creating, storing, or sharing information. This includes everything from devices (laptops, smartphones, printers, USB 'memory sticks') through to online services (citizen-facing online services, staff tools, corporate email).

Acceptable use of MHCLG IT

4. IT should help you to 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.

5. 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.

Personal use of MHCLG IT

6. Limited personal use of MHCLG 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.

7. It is recommended that you don't use your MHCLG email address for things that aren't work-related. You are able to use web-based email services such as GMail whilst at work on a department device.

Unacceptable use of MHCLG IT

8. 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.

9. 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
    - for example storing information on an internet file-sharing service like Dropbox without passwords
- excessive personal use during working time
- installing unlicensed or unauthorised software
- using departmental resources for any activity where you may be perceived to be speaking on behalf of the department when you are not doing so
    - for example, using a departmental email address to make personal representations in a planning process).

Why unacceptable use is a problem

10. Unacceptable use of IT might affect MHCLG 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

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

While you might be careful about acceptable use of MHCLG IT, there are still risks from malware, ransomware, or phishing attacks.

12. 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

13. If there is any doubt, or you are worried that the email might be malicious or inappropriate, report it immediately as an IT security incident.

Using MHCLG IT outside of MHCLG offices

14. Working wherever you need do so, not just in an MHCLG office, is an increasingly important need for you and the department. Most IT resources should be usable away from our offices but when doing so you must continue to ensure acceptable use of them.

15. You should also ask before taking MHCLG IT equipment outside the UK.

Using your own devices

16. You are able to use your own personal computer, tablet or smartphone to access some of the MHCLG services. You should make sure that your device is password protected, and that you don’t allow others to get access to MHCLG services on your device. You should also make sure that you don’t copy information from the MHCLG services into other software, or make copies onto your devices.

Avoid using removable media

17. Removable media like memory sticks are portable and easy-to-use. Unfortunately, this makes them a security risk, so avoid using them. If you feel that they are vital to your work, please get in touch with the Digital team.

On leaving MHCLG

18. All MHCLG equipment and data, for example laptops and mobile devices, must be returned to MHCLG when you leave the department’s employment.

19. All MHCLG data or intellectual property developed or gained during the period of employment remains the property of MHCLG and must not be retained beyond leaving or reused for any other purpose.