Ministry of Defence

JSP 740
Acceptable Use Policy (AUP) for Information and Communications Technology and Services

Part 1: Directive

The MOD Acceptable Use Policy

Scope

1. This Acceptable Use Policy (AUP) applies to everyone who uses any of the following for work or personal use:

   a. MOD devices, for example laptops, tablets, cameras and phones

   b. MOD systems and networks

   c. MOD provided Wi-Fi

   d. MOD communication channels such as email, instant messaging and voice calls

   e. MOD devices for any type of content capture, including videos and photographs

   f. All MOD provisioned IT services and software, including Internet and intranet

   (Referred to collectively in the following as MOD ICT)

2. This AUP applies if you are:

   a. performing Defence-related activities of any kind, including normal work, training, and official trade union business.

   b. on detached duty and using ICT supplied by another authority for your work for Defence, or if you are a contractor or occasional user of MOD-issued ICT.

   c. using welfare Wi-Fi provided for personal use on MOD premises.

3. If you break any of these rules, you may face disciplinary action or a criminal investigation.

General Rules for MOD ICT

4. When conducting MOD business, you must only use MOD-managed or MOD-approved devices and services. This includes software applications and generative AI tools.

5. When using MOD devices and services you must:

   a. use appropriate equipment in line with the classification of information, as well as additional sensitivities and handling requirements.

   b. use all ICT in accordance with Security Operating Procedures (SyOPs).

   c. ensure passwords, PINs and authentication devices and tokens (including smartcards) are protected and not shared.

   d. protect passwords at the highest level of the system to which they allow access.

e. make sure passwords are strong, not stored on personal devices and not re-used for private accounts.

f. change your password if you believe it has been compromised.

g. lock all screens whenever devices are left unattended.

h. adhere to rules about where PEDs and laptops can be used when on MOD establishments in accordance with (JSP 440 Part 2 Leaflet 4E).

General Behaviour

6. You **must not:**

a. request, create, access, store or send offensive, pornographic, indecent, or illegal material.

b. send information to, or work on MOD Information on your personal device[1].

c. breach copyright, licence agreements or data privacy rules, including but not limited to piracy and illegal streaming.

d. use any MOD ICT where it can be viewed, overheard, or overlooked by anyone not authorised to see it. This includes cameras, for example, public CCTV, household security cameras, vehicle cameras and microphones, Smart TVs, Smart speakers (e.g. Alexa) and technology embedded in user worn spectacles.

e. use MOD devices to capture QR codes of unknown origin or from MOD devices, except for Multi-Factor Authentication setup in line with JSP 440, Leaflet 5B.

f. remove, disable or change operational components, safety or security settings.

g. try to gain unauthorised access to information.

h. conceal information without authority.

i. release information without proper authority.

j. bring MOD into disrepute or obstruct its business.

k. be negligent in protecting MOD devices and services or the information you access.

l. break the law[2], or encourage or enable others to break the law.

m. travel outside the UK with a MOD-managed device unless for work purposes and with the appropriate permissions.

[1] The use of personal devices for multi-factor authentication is permitted. If the personal device is compromised a SIRF must be raised. This will not lead to an investigation of the personal device, it is for advisory purposes so that the authenticator application from that device can be disabled.
[2] Unless, in exceptional cases, your role and Terms of Reference have been authorised as one where a specific exemption stipulated in current legislation is applied.

Personal use of MOD ICT

7. The MOD does not accept any liability for any loss, damage, or inconvenience you may suffer as a result of personal use of MOD-issued ICT.

8. You may use MOD-issued equipment for limited personal use[3], however you **must not**:

a. use any MOD equipment as a replacement for a personal device.

b. take part in or promote personal commercial activity, including single or multi-level marketing.

c. undertake any or promote share dealing, crowdfunding or fundraising (unless MOD supported).

d. take part in or promote any gambling or lottery (except those run by Defence and CSSC and Single Service sports lotteries).

e. take part in or promote petitions or political campaigns.

f. use any password you have used for work to sign up to public websites or services.

g. use any MOD-specific information (for example, MOD email address or PUID), if signing up for websites and services for personal use.

h. undertake any form of crypto mining or use the device for hard wallet storage of cryptocurrency and/or keys.

i. use MOD services and processing power for anything other than its intended use.

Personal use: Telephony

9. You may use MOD telephones (desk phones, mobile phones and voice calls on laptops) for personal calls on the following occasions:

a. in an emergency.

b. you need to change personal arrangements because of unexpected work commitments.

c. you are away from your normal place of work and it is not practical to wait until you return home (calls within the UK only and keep them as brief as possible to convey the necessary information).

d. for inbound personal calls.

e. personal calls from outside the UK are permitted for emergency use only (unless local rules or orders apply).

[3] Although this can be stopped at any time at the MOD's discretion.

Emails

10. You **must not**:

a. configure email to auto-forward or create rules to bulk-forward mail to non-MOD email addresses.

b. transmit SPAM (electronic junk mail) or chain mail.

c. list non-work, or an individual person's MOD email addresses in external out of office notifications[4].

Social media, Internet and AI tools

11. You **must not**:

a. share or confirm any information about your own or anyone else's security clearance on social media or messaging apps.

b. share, confirm or discuss MOD business, including command and control activities or any discussion leading to decisions, on personal social media accounts or messaging apps.

c. record, livestream, distribute or forward images, video, messages, or data that will likely bring the MOD into disrepute.

d. share or confirm on social media any information classified above OFFICIAL.

e. share or confirm on social media any information that compromises the operational security or personnel security of MOD or its allies.

f. download or interact with any suspicious links or attachments received.

g. promote a charity cause not supported by Defence; personnel must use profiles that are their own private accounts not connected to their MOD roles.

12. You **must not** enter MOD information into public Internet-facing search engines or AI apps and tools.

13. If using generative AI as a productivity aid for work purposes, only use tools provisioned or authorised by MOD.

Messaging apps such as WhatsApp or Signal

14. Closed messaging apps are permitted on MOD-issued devices for keeping in touch purposes only (for example, letting colleagues know you are running late.)

15. Messaging Groups. All personnel should take care to understand who is in their messaging groups. They should also regularly review this list to ensure that any persons who no longer need access to the information are removed.

[4] For more information, see JSP 441: Using out of office (OOO) notifications effectively

16. Closed messaging apps must not be used to share or confirm any information classified above OFFICIAL, or any information covered in the paragraph above on Social Media.[5]

Devices, Systems and Networks

17. You **must not**:

a. connect unauthorised devices to MOD ICT or networks, including but not limited to MOD-issued or personal mobile devices, vaping devices, wearables, and gaming consoles for any reason including charging.

b. use public USB charging ports.

c. connect MOD-issued mobile devices to unauthorised computers.

d. connect MOD-issued or personal mobile devices to MOD ICT devices via a wireless connection other than to use the mobile hotspot.

e. connect personal mobile devices to MOD ICT via Bluetooth, only MOD provided peripherals may be connected.

f. download, use, store or distribute software or unauthorised[6] applications.

g. attempt to misuse, gain unauthorised access to (or prevent legitimate access to) any equipment, network, system, service, or account.

h. sync your MOD phone contacts to shared vehicles, including MOD fleet vehicles and MOD-provided hire cars.

Working from Home

18. When working from home, you **must not**:

a. connect any private wireless or Bluetooth equipment (including headsets, keyboards and speakers).

b. connect any private printers, Smart TVs or Smart monitors.

c. use tools on your private device to target any MOD device connected to a non-MOD network.

19. When working from home on a MODNET OFFICIAL laptop you may:

a. connect your personal screen using VGA, HDMI or DisplayPort wired connection.

b. connect a wired personal keyboard and wired mouse via a USB connection.

20. Do not connect any item of ICT equipment to your MOD laptop if you have security concerns about it.

[5] For more information, see JSP 441: Using Non-Corporate Communication Channels
[6] For further information see: Ordering Defence Digital Services.

Monitoring of MOD-issued ICT

21. The MOD monitors its ICT and networks. More information about the personal data held by the MOD can be found in the MOD privacy notice.

Reporting Incidents

22. You must report any activity that you think is in breach of the rules in this guidance via a Security Incident Report Form (SIRF).

23. You **must not** remove any personal data after being told your MOD-issued device is the subject of an investigation nor must you delay the return of that device when asked to do so by the MOD investigating authority.

Coherence with other Policy and Guidance

24. You must abide by the Security Operating Procedures (SyOPs) for the equipment you are using. You must also follow JSP 440 and 441, the MOD Corporate Standards Guide and your Service Code of Conduct at all times.

Related JSP	Title
JSP 440	The Defence Manual of Security
JSP 441	Information, Knowledge, Digital and Data in Defence

Further Advice and Feedback – Contacts

25. Comments, queries and feedback are welcome via the Cyber Defence and Risk (CyDR) Governance, Risk and Compliance (GRC) Policy Team.

Equality Analysis Statement

This JSP has been Equality Analysis Impact Assessed in accordance with the Department's Equality Analysis Impact Assessment (EQIA) Tool against: Part 1 - Assessment only, no diversity impact found.

The policy is due for review in September 2027.

Welsh Language Analysis Statement

This JSP has been assessed for its impact on the Welsh language and the Welsh-speaking public in Wales, in accordance with the Department's Devolved Assemblies Impact Assessment; no impact has been found.

Copyright Statement