Ministry of Defence

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

Part 1: Directive

Foreword

Across Defence we must make professional, legal and appropriate use of our Information and Communications Technology and Services (ICT&S). This means protecting our networks and our information, accounting for our actions, and ensuring that taxpayers' money is properly spent.

This Acceptable Use Policy (AUP), JSP 740, sets out clear rules for what you may and may not do on MOD-issued ICT&S, and includes a reminder of key rules for personal social media use. It makes clear the behaviours required which will help you to protect yourself and your colleagues, as well as MOD ICT&S and reputation, and ensure that there is clear accountability. If you break any of the rules in this AUP, you may find yourself facing disciplinary action, or, in the most serious cases, criminal investigation.

All Defence personnel must adhere to this Acceptable Use Policy. It is short, but very important.

Laurence Lee
Second Permanent Secretary

Preface

How to use this JSP

1. JSP 740 contains the rules on the acceptable use of all MOD-issued ICT&S. This JSP will be reviewed at least annually.

2. The JSP is structured in one part – a Part 1 Directive – that covers all use, including personal use, of MOD-issued ICT&S, and MOD-funded Wi-Fi, MOD telephones, devices, systems and networks. It contains a set of rules stating what users must not knowingly do when using MOD-issued ICT&S. This includes actions that are unlawful or illegal, and additional rules so that users comply with the Manual of Service Law, Queen's Regulations, and the Civil Service Code, including breach of confidence, as well as restrictions imposed by the Department.

Coherence with other Policy and Guidance

3. Where applicable, this document contains links to other relevant JSPs, some of which may be published by different Functions. Where particular dependencies exist, these other Functions have been consulted in the formulation of the policy and guidance detailed in this publication.

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

Training

4. There is no specific training on the AUP but it is included in the General Security Briefing, Information Management and Information and Cyber Security training available online in the Defence Learning Environment.

Further Advice and Feedback – Contacts

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

The MOD Acceptable Use Policy

Contents

When and where does the Acceptable Use Policy apply?

1. The MOD provides and issues Information and Communications Technology and Services (ICT&S) for Defence-related activities of all kinds, including normal work, training, and official trade union business. Limited personal use is also permitted. Whenever you use ICT&S owned, operated or issued by the MOD, you must do so responsibly in accordance with this policy.

2. This Acceptable Use Policy (AUP) applies to everyone (military and civilian) at all times when using MOD-issued ICT&S. It also applies if you are on detached duty, and using ICT&S supplied by another authority for your work for Defence or are a contractor or occasional user of MOD-issued ICT&S.

3. This AUP applies to use of all MOD-issued ICT&S. In addition to MOD-issued computers (including laptops), tablets, and phones, this includes all information systems, hardware, software, channels of communication including telephone, video, email, instant messaging, internet and intranet, Wi-Fi facilities and other MOD-provided services.

4. You must abide by this AUP, as well as the Security Operating Procedures (SyOPs) for the equipment you're using. You must also follow JSP 440, the MOD Corporate Standards Guide and your Service Code of Conduct at all times.

General Rules for MOD ICT&S

5. You **must**:

- only use MOD-managed or MOD-approved devices and services to conduct MOD business.

- use all ICT&S in accordance with Security Operating Procedures (SyOPs).

- apply good security behaviours in order to prevent and identify potential information or cyber security incidents and events.

- use appropriate ICT&S in line with the classification of information and follow guidance on specific sensitivities and handling requirements.

- ensure passwords, PINs and other authentication devices (including smartcards, multi factor authentication keys and other access tokens) are appropriately protected and not shared, and that any passwords are strong and unique, protected at the highest level of the system they give access to and not stored on personal devices.

- lock all device screens whenever devices are left unattended.

- adhere to the requirements relating to Information Protection Zones, including the use of Portable Electronic Devices (PEDs); see JSP 440 Part 2 Leaflet 4E.

6. You **must not** knowingly:

- offend, insult, harass, threaten or deceive other people.

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

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

- remove, disable, nullify or modify operational components, safety or security measures in MOD ICT, even when doing so allows you to re-establish or maintain your ability to work on MOD business.

- try to gain unauthorised access to, or conceal without authority, information, or release information without proper authority.

- bring MOD into disrepute or obstruct its business.

- be negligent in protecting the ICT&S, or the information you can access from it.

- break the law, unless your role and associated Terms of Reference have been authorised as one where a specific exemption stipulated in current legislation has been applied.

- encourage or enable others to break the law.

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

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

- use open-source Large Language Models (LLMs, e.g. ChatGPT) unless your business area has been specifically authorised to do so.

Personal use of MOD-issued ICT&S, including MOD-funded Wi-Fi and MOD Telephones

7. MOD allows you limited personal use of its issued ICT&S (although this can be stopped at any time at the MOD's discretion). MOD-issued ICT&S is not intended to replace your personal device. You are permitted to make personal purchases from websites, except where these would be prohibited by other rules within this AUP. Where this activity requires

a username/password combination, the details must not contain any MOD-specific information, e.g. your PUID.

8. 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&S. The MOD monitors its networks, so if you want to keep your personal information private, only use MOD-issued ICT&S for work.

9. When making personal use of MOD ICT&S you **must** comply with all other rules outlined in this document.

10. Additionally, when making personal use of MOD ICT&S, you **must not**:

- take part in personal commercial activity, including, but not limited to, single, network, direct referral, or multilevel marketing.

- undertake any form of share-dealing.

- undertake any form of crowdfunding or raise funds for individuals or charities, not formally supported by Defence.

- take part in any gambling or lottery (except that you may participate in one of the four lotteries run by Defence and the CSSC to support sporting facilities – the RN & RM, the Army, and the RAF Sports Lotteries, and the CSSC Lottery).

- take part in petitions, campaigns, politics or similar activity.

- waste MOD time, money or resources.

- use any password used to secure a MOD issued account to sign up to public websites or services. MOD email addresses should only be used to sign up to public websites or services where there is a justifiable business need, refer to JSP 441 - Participating safely in external communities for further guidance.

- undertake any form of crypto mining or use MOD services and processing power for anything other than its intended use.

11. When using MOD-funded Wi-Fi on personal devices or other MOD ICT provided for private use, you must adhere to the MOD Acceptable Use Policy and any specified Terms and Conditions. This includes the use of welfare Wi-Fi provided for personal use on MOD premises.

12. You may use MOD telephones for personal calls on the following occasions:

- in an emergency.

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

- if 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 brief).

- for inbound personal phone calls (but again keep them brief).

13. Otherwise, you should use your own phone so that you bear the cost of the call, not the MOD. In general, personal calls to or from locations outside the UK are only permitted for emergency use (unless local rules apply).

Social Media

14. *Social Media*. MOD security policy on social media can be found in JSP 440 Part 2 Leaflet 5A. The key messages for all personnel are summarised here.

15. You **must not** knowingly:

- share or confirm any information about your own or anyone else's security clearance online, including on social media and instant messaging services, either directly or through association with other user groups.

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

- share or confirm on social media any information classified above OFFICIAL. Any information that is marked or should be considered OFFICIAL-SENSITIVE, or that compromises the Operational Security[1] (OPSEC), Personal Security[2] (PERSEC) of MOD personnel or our allies, or the security of MOD in general, **must not** be shared or confirmed.

- download or interact with any suspicious links or attachments received on social media or instant messaging services.

16. *Messaging apps such as WhatsApp*. Messaging apps are permitted on MOD-issued devices for keeping in touch purposes only and **must not** be used to share or confirm any information classified above OFFICIAL, or any information covered in the paragraph above on Social Media. These may only be used where a MOD-provided solution is not available. See WhatsApp Guidance for further information.

Devices, Systems and Networks

17. You **must not** knowingly:

- 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, via a wired connection for any reason, including charging.

- connect MOD-issued mobile devices to unauthorised computers.

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

- connect MOD-issued or personal mobile devices to MOD ICT via Bluetooth.

---

[1] OPSEC is the process that gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of dispositions, capabilities and intentions of friendly forces. PJHQ SOP 9049 provides guidance on how to assess OPSEC risk.

[2] PERSEC refers to the duty of care MOD has to its personnel and personal security issues. PJHQ SOP 9050 provides guidance on how to assess PERSEC risk.

- download, use, store or distribute software or an application that is unauthorised, or which is not for a justified business purpose.

- try to misuse, gain unauthorised access to, or prevent legitimate access to, any ICT equipment, network, system, service or account.

Working from Home

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

- connect private or non-MOD issued wireless or Bluetooth devices or peripherals (e.g., headsets, keyboards, loudspeakers, hubs, switches, cameras etc) to MOD-issued devices.

- connect any private or non-MOD issued printer to MOD issued devices.

- use tools on your private devices or one belonging to a third party to target a MOD-issued device that is connected to a non-MOD network or standalone.

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

- connect your personal display screen (excluding Smart televisions or Smart monitors) to your MOD device using a VGA or HDMI wired connection. If you are prompted to install additional software for your device, you will NOT be able to use it.

- connect a wired personal keyboard and wired mouse by USB connection. Wireless mice and multi-functional mice (i.e. those used for gaming) are NOT to be connected.

If you have any security concerns over the authenticity of your screen, keyboard or mouse, DO NOT connect them.

Monitoring of MOD-issued ICT&S

20. The MOD monitors its ICT&S, including MOD-issued mobile phones, to help protect its information and its ICT&S, and to check that personnel are not breaking the law. Browsing history, malware and Wi-Fi connections are monitored and recorded to protect personal data and the wider network from malicious threats. Personal data collected during monitoring will only be used for the purpose for which it was gathered, and any further processing will be in accordance with the Data Protection Act 2018. More information about the personal data held by the MOD can be found in the MOD privacy notice.

Reporting Incidents

21. If you're aware of any activity that could be in breach of the rules here, then report it as soon as you can through your TLB Warning Advice and Reporting Point (WARP) to the Joint Security Coordination Centre (JSyCC) using the Security Incident Reporting Form (SIRF).

22. 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.

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 December 2023.

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