Ministry of Defence

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

Part 1: Directive

Foreword

In Defence, it is essential that we use our issued Information and Communications Technology (ICT) professionally and legally. We must protect our networks and our information, account for our actions, and ensure that taxpayers' money is properly spent.

This Acceptable Use Policy (AUP), JSP 740, defines what you may – and may not – do on MOD-issued ICT and services. 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.

The MOD allows us to make some personal use of its issued ICT, but we must avoid inappropriate cost to the MOD.

This Acceptable Use Policy is very short, but important.

There is a Part 1 only – no Part 2.

You are strongly advised to read the following pages and keep to the rules.

If in doubt, please seek advice within your unit, or contact the IRM team at UKStratCom DD-FI-IS-Info Policy (MULTIUSER).

Charlie Forte
Chief Information Officer
Ministry of Defence
January 2022

Preface

How to use this JSP

1. JSP 740 contains the rules on the acceptable use of MOD-issued Information and Communications Technology and Services (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 of MOD-issued ICT&S, including personal use, working from home, MOD-funded Wi-Fi and MOD telephones. It also contains a set of rules stating what users must not knowingly do when using MOD-issued ICT&S. This is divided into actions that are unlawful or illegal when using any ICT&S 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	Defence Manual of Security and Resilience

Training

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

Further Advice and Feedback – Contacts

5. Comments, queries and feedback are welcome via the IRM Team at UKStratCom DD-FI-IS-Info Policy (MULTIUSER).

The MOD Acceptable Use Policy

When and where does the Acceptable Use Policy apply?

1. The MOD provides and issues Information and Communications Technology (ICT) and services 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 and services owned, operated or issued by the MOD, you must do so responsibly.

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

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

Prohibited activities whenever using MOD ICT and services

4. 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 or licence agreements.
- connect unauthorised devices to MOD ICT or networks.
- connect MOD mobile devices to unauthorised computers.
- download, use, store or distribute software or an application that is unauthorised, not accredited for the system you are using or which is not for a justified business purpose.
- configure email to auto-forward or create rules to bulk-forward mail to non-MOD email addresses.
- 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 misuse, gain unauthorised access to, or prevent legitimate access to, any ICT equipment, network, system, service or account.
- try to gain unauthorised access to, or conceal without authority, information, or release information without proper authority.

- bring the MOD into disrepute or obstruct its business.

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

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

- encourage or enable others to break the law.

5. 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 etc) to MOD-issued devices.

- you must NOT knowingly connect any private or non-MOD issued printer to MOD-issued devices.

- you must NOT knowingly 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.

6. When working from home on a MODNET OFFICIAL laptop, exceptionally, while Covid-19 home working measures remain in place, you may:

- connect your personal display screen (excluding Smart televisions or Smart monitors) to your MOD device using a VGA or HDMI any wired connection supported by your device; 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.

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

Personal use of MOD ICT – Additional Rules

7. The MOD allows you limited personal use of its issued ICT (although this can be stopped at any time at the MOD's discretion). MOD-issued ICT is not intended to replace your personal device. You are permitted to make personal purchases from websites, except where the activity is prohibited, see the section above – 'Prohibited activities whenever using MOD ICT and services'. Where this activity requires a username/password combination, the details must not contain any MOD-specific information.

8. When making personal use of MOD ICT, 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 to support sporting facilities – the RN & RM, the Army, and the RAF Sports Lotteries, and the MOD 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.

9. The MOD does not accept any liability for any loss, damage or inconvenience you may suffer as a result of personal use of its ICT and services. The MOD monitors its networks, so if you don't want it to see your private information, only use its ICT for work.

MOD-funded Wi-Fi and other ICT equipment and services provided for private use

10. When using MOD-funded Wi-Fi on personal devices or other MOD ICT provided for private use, the MOD Acceptable Use Policy applies and you should also adhere to any specified Terms and Conditions.

Using MOD telephones for personal calls

11. 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's 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).

12. Otherwise, you should use your own phone or use a charging card 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).

Reporting Incidents

13. If you're aware of any activity that could be in breach of the rules here, then report it as soon as you can:

- to anyone in your management chain, or to the Senior Information Officer, Information Manager or Security Officer within your unit.
- to your TLB's WARP (Warning, Advice and Reporting Point).
- to the SPOC.

14. 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.

Monitoring of MOD ICT

15. The MOD monitors its ICT to help protect its information and its ICT, and to check that personnel are not breaking the law. 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.

Equality Analysis Statement

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

The policy is due for review in December 2022.

Welsh Language Analysis Statement

Welsh Language Analysis: 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