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 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's 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 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 my Information Policy team.

Charlie Forte
Chief Information Officer
Defence Authority for Information
December 2018

Preface

How to use this JSP

1. JSP 740 contains the rules on the acceptable use of MOD 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 the Department's ICT&S, including personal use, MOD Wi-Fi and MOD telephones. It also contains a set of rules stating what users must not knowingly do when using MOD 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 Defence Authority Policy and Guidance

3. Where applicable, this document contains links to other relevant JSPs, some of which may be published by different Defence Authorities. Where particular dependencies exist, these other Defence Authorities 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, Resilience and Business Continuity

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 this email address, or via the Information Portal on defnet.

The MOD Acceptable Use Policy

When and where does the Acceptable Use Policy apply?

1. The MOD provides 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 or operated 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 the MOD's 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 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 or illegal 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 applications that are unauthorised or not accredited for the system you are using.
- configure email to auto-forward or create rules to bulk-forward mail to non-MOD email addresses.
- remove, disable or nullify operational components, safety or security measures in MOD ICT.
- 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 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 has been authorised as one where a specific exemption stipulated in current legislation has been applied.

- encourage others to break the law.

Personal use of MOD ICT – Additional Rules

5. The MOD allows you limited personal use of its ICT (although this can be stopped at any time at the MOD's discretion). You are permitted to make personal purchases from websites (except auction sites). Where this activity requires a username/password combination, the details provided must not contain any MOD-specific information.

6. When making personal use of MOD ICT, you must not:

- take part in personal commercial activity, including, but not limited to, peer-to-peer marketing.

- undertake any form of share-dealing.

- 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 MOD email address to sign up to public websites or services.

7. 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 Wi-Fi and other ICT equipment and services provided for private use

8. When using Wi-Fi provided by the MOD for use with personally-owned devices, or other MOD ICT provided specifically for private use, always follow any Terms and Conditions. The section above – 'Prohibited activities whenever using MOD ICT and services' – applies (it will help you stay within the law).

Using MOD Telephones for Personal Calls

9. 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).

10. 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

11. 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.

Monitoring of MOD ICT

12. 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 2019.

Copyright Statement