IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

DWP Acceptable Use Policy

Version 2.5

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change
2.5	27/06/2018	

Updating policy

This policy will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

Introduction 4
Purpose 4
Scope 4
Who this policy applies to 4
Acceptable use principles 4
1. General principles 4
2. User IDs and passwords 5
3. Managing and protecting information 5
4. Personal use of DWP IT 6
5. Email/fax/voice communication 7
6. Websites and Social Media 7
7. Devices, systems and networks 8
8. Physical Security 9
9. Compliance 9

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Introduction

Information technology resources, such as PCs, laptops, Blackberrys, tablet devices and smart phones offer new and exciting ways of working and engaging with our colleagues and citizens. However, we must also be aware that improper use can impact us, our colleagues, citizens, DWP's reputation and the public purse.

This Acceptable Use Policy (AUP) aims to protect all users of DWP equipment and minimise such risks by providing clarity on the behaviours expected and required by DWP and the consequences of breaching the AUP. It sets a framework within which to conduct the DWPs business and explains how we can achieve compliance and evaluation of new business and technology requirements.

This policy replaces the Electronic Media Policy and is effective from 12 September 2016.

Purpose

To ensure that users understand their responsibility for the appropriate use of DWP's information technology resources. Understanding this will help users to protect themselves and DWP's equipment, information and reputation.

Scope

All DWP equipment and information (all information systems, hardware, software and channels of communication, including voice- telephony, social media, video, email, instant messaging, internet and intranet). User's personal information which is processed by DWP equipment is also subject to this policy.

Who this policy applies to

All DWP employees, agents, contractors, consultants and business partners (referred to in this document as 'users') with access to DWP's information and information systems.

Acceptable use principles

1. General principles

Users will:

1.1 Confirm prior to use of DWP equipment or information, and through use of the DWP security code of conduct that they agree to this AUP and understand that breaching this policy may result in disciplinary procedures.

1.2 Be responsible for their own actions and act responsibly and professionally, following the DWP Standards of Behaviour and respecting the Department and fellow employees, suppliers, partners, citizens.

1.3 Use information, systems and equipment in line with DWP security and Information Management policies

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

1.4 Immediately report any breach of this Acceptable Use Policy to their line manager and to the Security Advice Centre, and comply with official procedures when a breach of the policy is suspected or reported.

1.5 Never undertake illegal activity, or any activity that would be harmful to DWP's reputation or jeopardise staff and/or citizen data, on DWP technology.

1.6 Understand that both business and personal use will be monitored as appropriate

1.7 Be aware that they can use whistleblowing and raising a concern if it is believed that someone is misusing DWP information or electronic equipment.

1.8 Undertake education and awareness on security and using DWP information and technology, including the annual security e-learning, in order to be able to understand, recognise, and report threats, risks and incidents.

2. User IDs and passwords
Users will:

2.1 Protect user names, staff numbers, smart cards and passwords appropriately

2.2 Create secure passwords following best practice guidance.

2.3 Not logon to any DWP systems using another user's credentials.

2.4 Remove their network access smart card and/or lock the screen when leaving temporarily devices that are in use.

2.5 Log out of all computer devices connected to DWP's internal network during non-working hours.

3. Managing and protecting information
Users will:

3.1 Understand that they and DWP have a legal responsibility to protect personal and sensitive information.

3.2 Ensure that all information is created, used, shared and disposed of in line with business need and in compliance with the Information Management Policy, Information Asset Inventory guidance.

3.3 Not attempt to access personal data unless there is a valid business need that is appropriate to your job role.

3.4 Comply with Managing HR records in respect of handling employee information.

3.5 Not provide information in response to callers or e-mails whose identity they cannot verify.

3.6 Be careful not to be overheard or overlooked in public areas when conducting DWP business.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

3.7 Apply the Government Classification policy appropriately to document headers and email subject lines in relation to the Official-Sensitive handling caveat.

3.8 Not attempt to access, amend, damage, delete or disseminate another person's files, emails, communications or data without the appropriate authority.

3.9 Not attempt to compromise or gain unauthorised access to DWP IT, telephony or content, or prevent legitimate access to it.

3.10 Comply with the DWP Security Code of Conduct in managing DWP information.

4. Personal use of DWP IT
Users will:

4.1 Understand that they are personally accountable for what they do online and with DWP technology

4.2 Personal use of IT resources is permitted in an employee's own time when not on official duty or 'flexed on' as per the Flexible Working Hours Policy. Breaks taken in normal working hours, such as paid breaks, do not count as the employee's own time for personal use of DWP equipment.

4.3 Ensure that any personal information stored is appropriate i.e. legal, appropriate and compliant with this policy.

4.4 Understand that the ability to store personal information on DWP owned devices and systems is a privilege and DWP has a right to require the data is removed should this data interfere with business activity or use.

4.5 Ensure activities do not damage the reputation of DWP, its employees and citizens including accessing, storing, transmitting or distributing links to material that:

- Could embarrass or compromise DWP in any way;
- Is obtained in violation of copyright or used in breach of a licence agreement;
- Can be reasonably considered as harassment of, or insulting to, others;
- Is offensive, indecent or obscene including abusive images and literature.

4.6 Follow the DWP Standards of Behaviour and must not:

- Trade or canvass support for any organisation on official premises, whether it is for personal gain from any type of transaction or on behalf of external bodies.
- Send messages or material that solicit or promote religious, political or other non-business related causes, unless authorised by DWP.
- Provide unauthorised views or commitments that could appear to be on behalf of DWP.
- Undertake any form of gaming, lottery or, betting.
- Use any type of applications and/or devices to circumvent management or security controls.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

- Download software onto DWP devices with the exception of DWP supplied tablet devices and smart phones where permitted from an official source and appropriately licensed. This software must not compromise the performance or security of the device.
- Access personal webmail accounts on DWP equipment.
- Download music, video or other media-related files for non-business purposes or store such files on network drives.

5. Email/fax/voice communication
Users will:

5.1 Comply with the DWP's email policies

5.2 Only use appropriate language in messages, emails, faxes and recordings. Threatening, derogatory, abusive, indecent, obscene, racist, sexist or otherwise offensive content will not be tolerated

5.3 Not engage in mass transmission of unsolicited emails (SPAM).

5.4 Not alter the content of a third party's message when forwarding it unless authorised.

5.5 Not try to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned signatures).

5.6 Be vigilant to phishing emails and know how to spot and report suspicious emails

5.7 Only use your DWP email address for DWP business related activities and linked organisational activity (e.g. DWP discount schemes, CSL, Civil Service Jobs, HASSRA, etc.). When logging onto external web sites for personal use (e.g. for retail or internet banking purposes), DWP staff must use their personal email addresses. If you have already registered for personal services using your DWP email address you will not be disciplined but must try to change your personal details to register a personal email address as soon as possible

6. Websites and Social Media
Users will:

6.1 Only access appropriate content using DWP technology and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity, as described in the blocked categories list.

6.2 Report any access to a site that should be blocked by our web filters to their line manager and the Security Advice Centre.

6.3 Contact TechNow with requests to unblock a website (link is external) and do not attempt to bypass DWP web filters.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

6.4 Use social media appropriately by making themselves aware of the Social Media Policy and Cabinet Office guidelines.

6.5 Not put DWP information including anything that is sensitive / personal information onto online forums, blogs or social networking sites.

6.6 Only use approved DWP social media accounts for official business and where appropriate, use DWP branding and a professional image or persona on such accounts.

6.7 Be aware that their social media content may be available for anyone to see, indexed by Google and archived for posterity.

7. Devices, systems and networks

7.1 Only use systems, applications, software and devices which are approved, procured and configuration managed by DWP when undertaking official business, and apply DWP standards and guidance in their use.

7.2 Only use approved DWP devices connected to DWP network(s), including approved USBs, when undertaking official business.

7.3 Not connect DWP or personal mobile devices by USB cable to Departmental thin clients, thick clients, Surface Pro's, laptops or any other device connected to the Department’s infrastructure, for the purpose of uploading/ downloading files or charging.

7.4 DWP permits connecting DWP devices, laptops Surface pros etc., by WiFi (or Ethernet) to the internet to connect back to the department from anywhere e.g. home or a hotel. However DWP devices must not be connected to the internet via Captive Portals, for security reasons. DWP devices are set up so they do not connect to Captive Portals.

7.5 DWP permits wirelessly connecting a DWP Device to a DWP, or personal, mobile phone via a personal hotspot for the purpose of acquiring an internet connection (tethering) for work purposes. However, this feature is not currently available on any DWP iPhones due to technical limitations of the DWP implementation of the operating system. Tethering a personal mobile phone is permissible but DWP cannot be held liable for this use of a personal mobile phone including any data charges, and so any use of a personal phone for this purpose is the individual’s choice.

7.6 Ensure no official information is stored on devices without DWP security controls.

7.7 Do not use any personal wallpapers or screensavers.

7.8 Raise all software requests through Software Asset Management.

7.9 Seek exceptions to security policies by applying for an Exception.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7.10 DWP employees and contractors travelling outside the UK on official business and wishing to take DWP devices with them must contact the Personnel Security Team before they travel. DWP devices, including smart phones, must only be taken outside the UK when required for official business and approved by Personnel Security. DWP may prohibit the carrying and use of DWP devices in certain countries.

7.11 Employees and contractors are required to contact the Personnel Security team before travelling to certain countries, whether this is on official business or for a personal visit. Employees and contractors should check the Travel Abroad: Staff Advice and Notification intranet page to check whether this includes the country they are visiting.

8. Physical Security

Users will:

8.1 Be responsible for keeping all portable devices assigned to them safe and secure and immediately report any loss or damage of their equipment to their line manager and the Security Advice Centre.

8.2 Protect DWP equipment appropriately when travelling e.g.

- laptops must always be carried as hand luggage
- Never leave a portable device in sight in parked vehicles

8.3 Return all DWP equipment when leaving DWP. Line Managers must complete all appropriate exit procedures with leavers.

9. Compliance

9.1 If for any reason users are unable to comply with this policy or require use of technology which is outside its scope, this should be discussed with their line manager in the first instance and then the Security Advice Centre who can provide advice on escalation/exception routes.

9.2 All requests to use new software not currently approved by DWP must be subject to the Software Approvals process though the Security Advice Centre.

9.3 Line managers are responsible for ensuring that users understand their responsibilities and consequences as defined in this policy and continue to meet its requirements for the duration of their employment with DWP. They are also responsible for monitoring employees' ability to perform assigned security responsibilities. However, this does not remove responsibility from employees, they are responsible for ensuring that they too understand their responsibilities as defined in this policy and continue to meet the requirements. It is a line manager's responsibility to take appropriate action if individuals fail to comply with this policy.

9.4 Breaching this policy may result in disciplinary procedures (including criminal prosecution) which could lead to dismissal.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

9.5 DWP's Security and Resilience team will regularly assess for compliance with this policy, DWP Collaboration Services will use software filters to block access to some online websites and services in order to support compliance.