DWP Acceptable Use Policy

Introduction

The Acceptable Use Policy (AUP) aims to protect all users of DWP equipment and data and minimise risk by providing clarity on the behaviours expected and required by DWP employees, Agents, Service Providers, Contractors and Consultants. It sets a framework on how to conduct DWPs business to meet legal, contractual and regulatory requirements and defines how individuals must behave in order to comply with this policy.

Read the full policy, or jump to a specific section using the links below:

Purpose

To ensure that individuals understand their responsibilities for the appropriate use of DWP's information technology resources. Understanding what is expected will help individuals to protect themselves, colleagues and DWP's equipment, information and reputation and ensure that there is clear accountability.

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, suppliers and business partners (referred to in this document as ‘users’) with access to DWP’s information and information systems and assets.

Acceptable use principles

1. General principles

Users must:

1.1 Confirm prior to use of DWP equipment or information, that they agree to complying with 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 colleagues, suppliers, partners and citizens.

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

1.4 Immediately report any breach of this Acceptable Use Policy to their line manager and to the **Security Incident Response Team** 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 of DWP systems will be **monitored** as appropriate.

1.7 Understand that they can use **whistleblowing and raising a concern** if it is believed that someone is misusing DWP assets, information or electronic equipment.

1.8 Undertake education and awareness on security and using DWP information and technology, including the mandatory annual security e-learning, in order to support the understanding of recognising and reporting threats, risks, vulnerabilities and incidents.

2. User IDs and passwords

Users must:

2.1 Protect usernames, staff numbers, smart cards, dongles and passwords appropriately.

2.2 Create secure passwords following **How to create a Password or PIN.**

2.3 When using a password manager, ensure that their master password is stored securely in line with **Keeping your Passwords and PINs secure**. Passwords must not be stored in shared folders or written down.

2.4 Not log on to any DWP systems using another user's credentials.

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

2.6 Log out of all computer devices connected to DWP's internal network during non-working hours, i.e. at the end of the working day.

3. Managing and protecting information

Users must:

3.1 Understand that they and DWP have a legal responsibility to protect personal and sensitive information and must not misuse their official position to further private interests or those of others. The **Civil Service Code** Standards of Behaviour: Integrity refers.

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 and **Retention of Specific Information Guidance.**

3.3 Not attempt to access anyone's personal data unless there is a legitimate business need that is appropriate to their job role. Users must not, under any circumstances, knowingly access, or attempt to access, their own DWP records or the records of friends, family members, ex-partners, relatives or anyone else they know on any Departmental computer, paper file or benefit system, irrespective of motivation. **DWP Standards of Behaviour para 78 refers.**

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

3.5 Not provide information in response to any type of request whose identity they cannot verify.

3.6 Ensure they are not overheard or overlooked in public areas when conducting DWP business.

3.7 Apply the **DWP Security 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.

4. Non-Corporate Communications Channels

The use of Non-Corporate Communications Channels is strictly controlled.

4.1 SECRET or TOP SECRET information must never be communicated via NCCCs.

4.2 DWP customers should never be contacted via NCCCs.

4.3 Official Sensitive or other ‘significant information’ must only be communicated through NCCCs in exceptional circumstances and only with an approved Security Policy Exception. Significant information is information that materially impacts the direction of a piece of work or that gives evidence of a material change to a situation. Where such exceptions are granted, records of official business carried out via an NCCC must be transferred onto corporate systems (e.g., SharePoint) as soon as is practicably possible.

4.4 Logistical or other non-significant information can be accessed through NCCCs with due regard to an individual’s security responsibilities.

Guidance on the use of NCCCs can be found here: **Non-Corporate Communication Channels Guidance.**

5. Personal use of DWP IT

Users must:

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

5.2 Understand that DWP allows personal use of its IT resources in an employee’s own time when not on official duty or ‘flexed on’ as per the **Flexible Working Hours Policy**.

5.3 Ensure that any personal information stored is appropriate i.e., legal, applicable and compliant with this policy and GDPR legal requirements.

5.4 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.

5.5 Ensure personal 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, language and literature.

5.6 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.
- Use malicious, harassing, abusive or threatening communication.
- Incite hate, bullying and harassment.
- Visit pornographic sites or undertake any form of gaming, lottery or betting.
- Use behaviour that is discriminatory in any sense (e.g., on the grounds of sex, sexual orientation, gender, race, age, religious beliefs or disability).
- Use any type of applications and/or devices to circumvent management or security controls or damage, destroy, or deny availability of service.
- 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.

5.7 The DWP does not accept any liability for any loss, damage or inconvenience you may suffer as a result of personal use of its IT.

6. Email/fax/voice communication

Users must:

6.1 Comply with the DWP's **email policies.**

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

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

6.4 Not alter the content of a third party's message when forwarding it unless authorised to do so.

6.5 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).

6.6 Be vigilant to scam targeting communications especially **phishing** emails and know how to spot and report suspicious emails.

6.7 Employees and contractors must not use their DWP email address for personal use. 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, Trade Union activity and other officially provided Internet links). Please refer to the **DWP Email Policy**. All employees must use their personal email address for personal activities including purchasing and selling of goods, internet banking and any other personal activity, failure to comply may lead to disciplinary action.

7. Websites and Social Media

Users must:

7.1 Comply with the **Social Media Policy** and **Social Media Standards** and be aware of **Cabinet Office guidelines (link is external)**. They must use social media appropriately and understand that the principles covering the use of social media by civil servants in either their official or personal capacity are the same as those that apply for any other activity and that they are responsible for the content they post. Section 3 of Social Media Standards refer.

7.2 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.

7.3 Understand that their social media content/footprint may be available for anyone to see, indexed by Google and archived for posterity.

7.4 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.

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

7.6 Report any access to a site that should be blocked by our web filters to their line manager and contact DWP Place with a **request to block a website (link is external)**.

8. Devices, systems and networks

8.1 Only use systems, applications, software and devices (including USBs, laptops and smart phones), which are approved, procured and configuration managed by DWP when undertaking official business, and apply DWP standards and guidance in

their use. The installation and use of the TikTok application is restricted on all DWP devices and access must not be attempted.

8.2 Users with DWP mobile phones must always install the most up to date software when it becomes available as this ensures the device has the latest security updates installed and so remains fully compatible with DWP systems. Failure to do so may result in the device becoming restricted from accessing any DWP systems prior to potential withdrawal of the service.

8.3 When individuals are required to generate a two-factor authentication one-time password to access a DWP system, including enrolment and password reset by an authorised Windows Hello for Business user, use of a personal device is permitted in the absence of a DWP device.

8.4 The use of personal Bluetooth headsets, keyboards and mice are permitted when paired with DWP devices that are enabled to support the connectivity i.e. Windows 10, Smartphones and MacBooks. Bluetooth connection must be compatible with DWP devices and users must not download any software onto DWP devices to conduct the pairing of Bluetooth.

8.5 DWP permits the use of personal mobile phones and personal landline numbers for voice calls in exceptional circumstances only which include internal calls to colleagues within DWP, other Government Departments, Local Authorities and the supply chain/business partners however personal or sensitive information should not be discussed. Where a user has access to a DWP phone or a Softphone on their DWP device, these must be used as they are the department’s preferred method of communication. Employees and contractors must not use personal phones to contact customers or their appointed agents as this still remains prohibited. The use of other personal mobile phone functionality including SMS texting or personal Email for DWP work purposes is not permitted.

8.6 The limited use of personal devices (laptops, tablets etc.) is permitted when undertaking training courses for DWP work purposes, for example where access to training related material and examinations is restricted on DWP devices and proving difficult to access. This is not a mandatory solution but a personal choice when there is restricted access to training material and courses on DWP devices that prevents essential learning. The Department is not responsible for any damage, theft or introduction of malware to personal devices as a result of personal choice by individuals to use their own device for access to training materials. Individuals should take great care when using personal devices for training purposes, ensuring that any official information, that should not be in the public domain, must not be divulged nor exposed.

8.7 Users must not connect DWP or personal mobile devices by USB cable to Departmental 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.

8.8 DWP permits connecting DWP devices, laptops Surface pros etc., by Wi-Fi (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.

8.9 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. 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.

8.10 Users must ensure no official information is stored on devices without DWP security controls.

8.11 Do not use any personal wallpapers or screensavers. The use of personal background settings (e.g., **MS Teams (link is external)**), images (e.g., **Outlook profile**) etc. is permitted on DWP devices but must be respectful and must not contain any inappropriate or offensive material that may bring the individual or DWP into professional disrepute.

8.12 Raise all software requests through **Software Asset Management**.

8.13 Where accessible, users can use approved private Artificial Intelligence (AI) applications that sit within DWP systems.

8.14 Users must not attempt to access public AI applications (such as ChatGPT) when undertaking DWP business, or on DWP approved devices.

8.15 DWP employees and contractors travelling outside the UK on official business and wishing to take DWP devices with them should review the **HR guidance on working abroad** and must contact the **Personnel Security Team (link sends e-mail)** 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.

8.16 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 e.g., a holiday. Employees and contractors should check the **Travel Abroad: Staff Advice and Notification** intranet page to check whether this includes the country they are visiting.

9. Physical Security

Users must:

9.1 Comply with the DWP **Physical Security Policy** & **Physical Security Standards**

9.2 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 log a **security incident** using the **Security Incident Referral Webform**. If the device is a work phone/smart phone you must also complete a **Lost/Stolen Device Report (link is external)** form via DWP place and contact IT Support urgently on 0800 464 3549 to ask for the phone to be suspended.

9.3 Protect DWP equipment appropriately when travelling e.g.

- Laptops must always be carried as hand luggage.
- Never leave a portable device visible in parked vehicles.
- Never leave equipment unattended in a public place e.g., on public transport

9.4 Return all DWP assets when leaving DWP. Failure to return equipment could lead to steps being taken to recover the cost, which could include legal action through the civil courts. Line Managers must complete all appropriate **exit procedures** with leavers. See the **DWP Leaver Checklist** for more information.

10. Compliance

10.1 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.

10.2 Seek exceptions to security policies by applying for an **Exception.**

10.3 All requests to use new software not currently approved by DWP must be subject to the Software Approvals process though **Software Asset Management**.

10.4 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. This does not remove responsibility from employees, who must ensure that they too understand their responsibilities as outlined 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.

10.5 DWP actively monitors employee and contractor personal use of IT and equipment to ensure everyone is complying with this policy (AUP) and the **DWP Social Media Policy**. Monitoring complies with and respects the privacy rights of all employees as outlined in the **DWP Employee Privacy Notice**. The consequences of failing to comply with the personal use limitations of DWP IT and equipment are serious and attract disciplinary penalties up to and including dismissal.

10.6 DWP's Security and Data Protection Team will regularly assess for compliance with this policy and may need to inspect physical locations, technology systems,

design and processes and speak to people to facilitate this. All DWP employees, agents, contractors, consultants, business partners and service providers will be required to facilitate, support, and when necessary, participate in any such inspection. DWP Collaboration and Communication Services will use software filters to block access to some online websites and services.

10.7 Failure to **report a security incident**, potential or otherwise, could result in disciplinary action

10.8 Breaching this policy may result in disciplinary procedures which could lead to dismissal, including criminal prosecution.