DWP remote working security policy

1. Overview

1.1 For security purposes, remote working is identified as creating, accessing and processing, storing or handling departmental information anywhere outside of DWP business locations, including travelling on “official business” outside of the UK. This policy does not replace any legal or regulatory requirements, to which all DWP employees must comply.

2. Scope

2.1 This policy defines controls and preventative measures that protect and secure departmental information and assets when working away from an individual’s central office or normal place of work. This includes any remote location, including when travelling on public/private transport or working at home or shared space.

2.2 This policy relates to the handling of all DWP paper records, all DWP electronic devices/equipment that have the capability to create, transmit, receive, record, process or store DWP data/information.

2.3 This policy applies to all DWP “users” of departmental assets who are employees, contractors and anyone who handles, processes or stores DWP information, whilst working remotely. The relevant HR information should be read in conjunction with this policy and applies to individuals who:

- have a personal contractual “homeworking” arrangement with the appropriate approval and authorisation.
- have permission to work in remote environments daily, or on an “ad hoc” basis, e.g., hybrid working, in public areas, in hotels, or using any public or private transport in a work capacity, the examples are not exhaustive.

3. Policy statements

3.1 DWP colleagues must consider the sensitivity, classification and value of information being handled when working remotely and should understand the policy requirements on protecting government information and assets, managing them accordingly, including:

- only using systems, applications, software and devices (including USBs, laptops and mobile phones etc), which are approved, procured and configuration managed by DWP to undertake official business, and apply DWP standards and instructions in their use.
- consideration of classification and sensitivity of the information being worked on and whether it is appropriate to do so outside of a secure DWP working environment.
- ensuring that only essential documents or files be removed and handled/securely transported away from the office, obtaining line manager approval to do so where appropriate.
- not allowing any unauthorised personnel to access smartcards, access tokens, any departmental information, DWP approved portable devices or

other DWP approved desktop PCs.

- consider the sensitivity/classification of information and privacy requirements where smart devices/listening assistants are/may be present and active. This includes (but not limited to) Alexa, Siri, Google and Microsoft Cortana.
- individuals must be vigilant when using DWP information to reduce the risk of mishandling data which could lead to a security breach, particularly where remote working is in practice.
- report any security incident.
- store DWP information and assets securely, ensuring also the appropriate secure destruction of DWP printed information.

3.2 When in transit, staff must not leave any IT equipment or sensitive information (whether hardcopy or electronic) unattended at any time. If travelling by vehicle, IT equipment and information must be stored securely out of sight and removed whenever the mobile worker leaves the vehicle.

3.3 DWP employees and contractors are not permitted to work remotely overseas. Exceptional circumstances may be considered in line with Civil Service HR guidance and security risk. Employees required to travel outside the UK on official business with approval and permission to take any DWP device with them, must follow HR guidance and must always contact the appropriate team prior to travel. DWP devices, including mobile phones, must only be taken outside the UK when permitted/required for official business and approved by the relevant team. DWP prohibits the carrying and use of DWP devices in specific countries.

4. Accountabilities and responsibilities

4.1 The Chief Security Officer (CSO) is the accountable owner of the DWP Remote Working Security Policy. There is a team responsible for policy maintenance and review.

4.2 Line Managers are responsible for, and must ensure that:

- employees are made aware of the relevant Security Policies and HR Policies which support working securely in remote locations.
- equipment is appropriately authorised; departmental assets are accounted for, and a record maintained prior to issue and use of all DWP approved devices.
- employees are made aware of potential risks often associated with remote working e.g.
    - the loss or theft of IT equipment or sensitive and personal data.
    - the inadvertent or deliberate disclosure of sensitive, operational information.
    - unsecured storage of information and user credentials, such as username and passwords.
    - tampering, where IT equipment/information is left unattended.

4.3 Users must always:

- seek line management approval, prior to undertaking any type of remote working, including hybrid working and travelling for official business outside of the UK, the list is not exhaustive.

- take personal responsibility to understand and comply with relevant DWP security policies where circumstances are relevant.

5. Compliance

5.1 Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with DWP. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

5.2 All DWP employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with the line manager in the first instance for resolution

5.3 Where it is deemed necessary to request the consideration of an exception to policy, the process should be followed. Failure to comply with this policy may lead to disciplinary action and could result in serious consequences, including dismissal.

Supporting information is available and should be read in conjunction with this policy.