## Schedule 6 - Security Requirements and Plan

### 1 Introduction

1.1 This Schedule covers:

(a) Principles of security for the Contractor System, derived from the Security Policy, including without limitation principles of physical and information security;

(b) The creation of the Security Plan;

(c) Audit and testing of the Security Plan;

(d) Conformance to ISO/IEC:27002 (Information Security Code of Practice) and ISO/IEC 27001 (Information Security Requirements Specification) (Standard Specification); and

(e) Breaches of Security.

(f) Security provisions with which the Contractor shall comply in providing the services relevant to this Contract.

### 2 Principles of Security

2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of the Authority's Data.

2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:

(a) is in accordance with Good Industry Practice and Law;

(b) complies with the Security Policy;

(c) meets any specific security threats to the Contractor System;

(d) complies with ISO/IEC27002 and ISO/IEC27001 in accordance with paragraph 5 of this Schedule; and

(e) meets the requirements of the Cyber Essentials Scheme, unless deemed out of scope for this requirement.

2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to minimise the following risks:

(a) loss of integrity of Authority Data;

(b) loss of confidentiality of Authority Data;

(c) unauthorised access to, use of, or interference with Authority Data by any person or organisation;

(d) unauthorised access to network elements and buildings;

(e) use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data;

(f) loss of availability of Authority Data due to any failure or compromise of the Services; and

(g) loss of confidentiality, integrity and availability of Authority Data through Cyber/internet threats

## 3 Security Plan

### Introduction

3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period and after the end of the Contract Period in accordance with the Exit Management Strategy, which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule.

3.2 A draft Security Plan provided by the Contractor as part of its bid is set out in Appendix B.

### Development

3.3 Within twenty (20) Working Days after the Commencement Date and in accordance with paragraphs 3.10 to 3.12 (Amendment and Revision), the Contractor will prepare and deliver to the Authority for approval the full and final Security Plan which will be based on the draft Security Plan set out in Appendix B.

3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within then (10) Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause I2 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 of this schedule may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.9 shall be deemed to be reasonable.

### Content

3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:

(a) the provisions of this Contract; this Schedule (including the principles set out in paragraph 2);

(b) the provisions of Schedule 1 relating to security;

(c) ISO/IEC27002 and ISO/IEC27001;

(d) the data protection compliance guidance produced by the Authority.

3.6 The references to standards, guidance and policies set out in paragraph 3.5 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

3.7 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authority's Representative of such inconsistency immediately upon becoming aware of the same, and the Authority's Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.

3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001.

3.9 Where the Security Plan references any document which is not in the possession of the Authority, a copy of the document will be made available to the Authority upon request. The Security Plan shall be written in plain English in language which is readily comprehensible to the staff of the Contractor and the Authority engaged in the Services and shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule.

**Amendment and Revision**

3.10 The Security Plan will be fully reviewed and updated by the Contractor annually, or from time to time to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Contractor System, the Services and/or associated processes;

(c) any new perceived or changed threats to the Contractor System; and

(d) a reasonable request by the Authority.

3.11 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

3.12 Any change or amendment which the Contractor proposes to make to the Security Plan as a result of an Authority request or change to Schedule 1 or otherwise shall be subject to the change control procedure and shall not be implemented until approved in writing by the Authority.

## 4 Audit and Testing

4.1 The Contractor shall conduct tests of the processes and countermeasures contained in the Security Plan ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

4.2 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

4.3 Without prejudice to any other right of audit or access granted to the Authority pursuant to this Contract, the Authority shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Contractor's compliance with and implementation of the Security Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery Services. If such tests impact adversely on its ability to

deliver the Services to the agreed Service Levels, the Contractor shall be granted relief against any resultant under-performance for the period of the tests.

4.4 Where any Security Test carried out pursuant to paragraphs 4.2 or 4.3 above reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Authority's approval in accordance with paragraph 3.12, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with the Security Policy or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph 4, a weakness means vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

## 5 Compliance with ISO/IEC 27001

5.1 The Contractor shall carry out such regular security audits as may be required by the British Standards Institute in order to maintain delivery of the Services in compliance with security aspects of ISO 27001 and shall promptly provide to the Authority any associated security audit reports and shall otherwise notify the Authority of the results of such security audits.

5.2 If it is the Authority's reasonable opinion that compliance with the principles and practices of ISO 27001 is not being achieved by the Contractor, then the Authority shall notify the Contractor of the same and give the Contractor a reasonable time (having regard to the extent of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO 27001. If the Contractor does not become compliant within the required time then the Authority has the right to obtain an independent audit against these standards in whole or in part.

5.3 If, as a result of any such independent audit as described in paragraph 5.2 the Contractor is found to be non-compliant with the principles and practices of ISO 27001 then the Contractor shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Authority in obtaining such audit.

## 6 Breach of Security

6.1 Either party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.

6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall:

(a) immediately take all reasonable steps necessary to:

(i) remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and

(ii) prevent an equivalent breach in the future.

Such steps shall include any action or changes reasonably required by the Authority. In the event that such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under this Contract, then the Contractor shall be entitled to refer the matter to the change control procedure in clause F3 (Changes to the Contract).

(b) as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

**7 Authority Data relevant to the Contract**

7.1 The Specification will outline the Services to be provided by the Contractor, including the type of Authority Data involved.

7.2 The majority of information that is created or processed by the public sector is described as 'Official'. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media.

**Appendix A – DWP Security Policies and Standards**

1 The Department for Work and Pensions (DWP) treats information as a valuable asset and considers that it is essential that information must be protected, together with the systems, equipment and processes which support its use. These information assets may include data, text, drawings, diagrams, images or sounds in electronic, magnetic, optical or tangible media, together with any Personal Data for which DWP is the Controller.

2 In order to protect DWP information appropriately, our Contractors must provide the security measures and safeguards appropriate to the nature and use of the information. All Contractors of services to DWP must comply, and be able to demonstrate compliance, with the relevant DWP policies and standards.

3 The main DWP policies include:

- Information Security Policy;
- Physical Security Policy; and
- Acceptable Use Policy.

4 The above policies are attached as Appendices C, D and E to this Schedule.

5 Each Contractor must appoint a named officer who will act as a first point of contact with the Department for security issues. In addition, all staff working for the Contractor and where relevant Sub-contractors, with access to DWP IT Systems, Services, DWP information or DWP sites must be made aware of these requirements and must comply with them.

6 The policies and requirements are based on and follow ISO27001 and Cyber Essentials, but with specific reference to DWP use.

7 Whilst Departmental policies are written for internal Departmental requirements all Contractors must implement appropriate arrangements which ensure that the Department's information and any other Departmental assets are protected in accordance with prevailing statutory and government requirements. These arrangements will clearly vary according to the size of the organisation so should be applied proportionately.

8 It is the Contractor's responsibility to monitor compliance of any Sub-contractors and provide assurance to DWP as requested.

9 Failure to comply with any of these Policies and Standards could result in termination of current contract.

10 The following are some key basic requirements that all Contractors must apply:

(a) **Personnel Security**

(i) Staff recruitment in accordance with government requirements for pre-employment checks; including Baseline Personnel Security Standard.

(ii) Staff training and awareness of DWP security and any specific contract requirements.

(b) **Secure Information Handling and Transfers**

Physical and electronic handling, processing and transferring of DWP Data, including secure access to systems and the use of encryption where appropriate.

(c) **Portable Media**

The use of only encrypted laptops, encrypted storage devices and other protected removable media when handling DWP information.

(d) **Offshoring**

DWP data must not be processed outside the United Kingdom without the prior written consent of DWP and must at all times comply with the Data Protection Legislation.

(e) **Physical Security**

Security of premises and control of access.

(f) **Security Incidents**

Includes identification, managing and agreed reporting procedures for actual or suspected security breaches.

**Appendix B – Draft Security Plan**

# INTENSIVE PERSONALISED EMPLOYMENT SUPPORT (IPES)

**Appendix C - Information Security Policy**

**DWP INFORMATION SECURITY POLICY**

**Contents**



## Background

1.1 DWP is committed to ensuring that effective security arrangements are implemented and regularly reviewed to reduce the threats and manage risks to:

- The information that DWP collects, creates, uses and stores,
- DWP employees, claimants and citizens,
- DWP's physical assets and resources,
- DWP's digital, IT and communication systems, and
- Premises that DWP uses to accommodate its operations, people, and visitors

## Scope

2.1 This overarching policy provides direction for all DWP information security policy and the standards and controls which underpin it.

2.2 This policy aligns with and is based on the ISO 27000 series and in particular ISO27001 techniques and principles and ISO27002 requirements and will be used to inform DWP future consideration of an Information Security Management System. Standards drawn from the ISO 27000 series will be applied and communicated as needed.

2.3 This policy applies to all aspects of cyber and information security, including the specification, design, development, installation, operation, connection, use and decommissioning of the systems, services and equipment used to store, process, transmit or receive information.

2.4 This policy applies to all DWP data, and any data that DWP is processing for other Controllers.

2.5 This policy applies to:

- All DWP employees - who should understand their responsibilities in using the Department's information assets including its systems. DWP Employee non-compliance with this policy may result in disciplinary consequences.

- DWP staff engaged in designing and implementing new technology solutions, who must reflect the policy requirements into design and build.

- DWP Contracted suppliers that handle/access/process Authority Data. Contracted suppliers must provide the security measures and safeguards appropriate to the nature and use of the information. All Contracted suppliers of services to the DWP must comply, and be able to demonstrate compliance, with the Department's relevant policies and standards.

**Accountabilities**

3.1 The Chief Security Officer is the accountable owner of the DWP Information Security Policy and is responsible for its maintenance and review, through the Head of Security Policy, Governance & Resilience.

3.2 Any exception to the Information Security Policy must be risk assessed and agreed by the Chief Security Officer.

**Policy Statements**

4.1 DWP recognises all information has value and sets out in this Information Security Policy how it safeguards DWP information through security standards, and protects the systems, equipment and processes that support its use through applying controls and a control environment.

4.2 This Information Security Policy defines how we achieve information security through implementing supporting standards and controls to protect information;

- Confidentiality: by restricting access to authorised users;

- Integrity: by making sure that the information is always accurate and complete;

- Availability: by making sure that the information is available to authorised users when required.

4.3 DWP protects its systems and processes through standards that are applied proportionately, based on formal risk assessments, continually reviewed, and aligns with the following:

- The Data Protection Legislation and the HMG Security Policy Framework.

- Related HMG standards and Good Practice Guidance for protecting personal data and managing information risk including those of CESG.

- The ISO27001 techniques standard, the ISO27002 code of practice, and other ISO 27000 standards and security best practice.

- Contractual obligations

- Relevant Codes of Connection.

- Other applicable legislation.

4.4 DWP requires Contracted Suppliers that generate, access and process Authority Data to take a similar proportionate, risk based approach to information security in

accordance with the relevant DWP Security Policies and Standards which adopt and apply ISO 27001 Standards and the Cyber Essentials.

4.5 DWP applies the Baseline Personnel Security Standard (BPSS) in employee recruitment and requires Contracted Suppliers to apply similar or identical controls where applicable. DWP applies Human Resources policies in the protection of its information and requires Contracted Suppliers apply similar personnel security policies.

4.6 DWP will ensure that DWP and its suppliers implement and operate information security in accordance with the organisational standards and procedures to mitigate against breaches of legal, statutory, and embed contractual obligations related to information security.

4.7 DWP systematically monitors and measures information security performance against its own and cross government metrics. DWP develops and improves information security policies and standards to provide sufficient protection for information by addressing identified risks, and consistent with central HMG standards and guidance. New information security standards and procedures will be communicated to employees and others on a regular basis.

**Responsibilities**

5.1 DWP's Information Security Policies and Standards provide appropriate protection for personal and sensitive personal data as a result of effective implementation of the following responsibilities:

*5.1.1 Governance and Compliance Functions*

5.1.1.1 Enable management of information security through developing governance structures in an organisation that directs and manages information security,

5.1.1.2 Provide control of information security risks within DWP to acceptable levels by risk management and the use of protective marking and other controls,

5.1.1.3 Support DWP employees to comply with these requirements, as expressed through the HR Standards of Behaviours and Security Code of Conduct, and ensure employees are aware of the consequences of non-compliance,

5.1.1.4 Ensure that suppliers are aware that failure to comply with this policy and other requirements (which will be communicated through the contractual process) will result in corrective action and escalation following agreed processes.

*5.1.2 Line Managers and Contracted Suppliers*

5.1.2.1 Ensure all employees fully understand and fulfil their agreed responsibilities for information security under the Security Code of Conduct and the Acceptable Use Policy,

5.1.2.2 Require Contracted Suppliers to be aware of and fulfil their information responsibilities including personnel information security responsibilities,

5.1.2.3 Monitor the actions of system and service users to identify individual responsibility for information security,

*5.1.3 Information Asset responsibility*

5.1.3.1 Identify DWP information assets and define responsibilities to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation and to the citizen, and its hosting location,

5.1.3.2 Ensure DWP has appropriate structures and processes to enable the Department to understand the use of and monitor its information assets.

*5.1.4 Employees and Contracted Suppliers - access to information assets and systems*

5.1.4.1 Ensure there are documented information asset access controls and procedures, and that security responsibilities have been allocated and accepted.

5.1.4.2 Ensure the effective use of cryptography, especially where interconnections between systems or services exist.

5.1.4.3 Ensure users are accountable for safeguarding their authentication information,

5.1.4.4 Ensure correct and secure operations of information processing facilities by regulating, monitoring and reviewing the implementation of protective measures,

5.1.4.5 Ensure the protection of information in networks and any supporting information processing facilities, and maintain the security of information transferred within an organisation and with any external entity,

5.1.4.6 Ensure personally identifiable information is not saved or processed in any spread-sheet or system other than those approved by DWP Security for that purpose. Personally identifiable information must only be placed in document frameworks such as MS Word, Excel and PowerPoint when following approved local business processes which apply DWP security policy,

5.1.4.7 Ensure that information security is integral to information systems across the entire lifecycle of acquisition, development, maintenance and decommissioning,

5.1.4.8 Define security responsibilities through contract terms and requirements for all suppliers to ensure protection of the organisation's assets that are accessible by suppliers,

*5.1.5 Security incident management function*

5.1.5.1 Define formal procedures for the management of information security incidents, including improvements and changes to those procedures,

*5.1.6 Continuity and Resilience function*

5.1.6.1 Require business units to develop, implement and embed appropriate information security business continuity management, including business continuity plans for critical systems and services to minimise disruption against identified threats and risks,

*5.1.7 Technology function (through Infrastructure Operations)*

5.1.7.1 Require disaster recovery functionality for security systems based on a business impact analysis, risk assessment and cost calculation and in compliance with ISO27001 to re-establish access to and protection of our information.

**Appendix D - Physical Security Policy**

**DWP PHYSICAL SECURITY POLICY**

**Contents**



## Audience

1.1 This DWP Physical Security policy applies to all DWP employees, contractors, partners, service providers and includes employees of other organisations who are based on DWP premises.

1.2 This policy does not apply to DWP staff operating out of sites owned and/or managed by other public bodies.

## Policy Objective

2.1 This provides our employees, contractors, partners and other interested parties with a clear policy direction that requires them to protect DWP premises and assets, and ensure that all necessary physical protective security measures are in place to prevent unauthorised access, damage and interference to DWP's assets and the occupants of its premises.

## Scope and Definition

3.1 Physical Security refers to measures that are designed to protect physical locations and the assets, information and personnel contained within.

3.2 This policy sets out the approach to be adopted to manage, develop, improve and assure Physical Security across DWP.

3.3 It is essential that our business is conducted in an environment where potential threats to DWP assets, information and personnel (including from terrorism, theft and insider threat actors) have been identified, risk assessed and appropriately mitigated to prevent interference, loss or compromise. This includes ensuring physical perimeters are protected and entry controls are in place to provide proportionate protection against natural disasters and terrorist attacks.

## Context

4.1 This policy sets out a framework to follow a 'layered' approach to physical security. It provides suitably secure environments from which DWP can operate to achieve its strategic aims and objectives by implementing security measures in layers, to appropriately protect personnel and DWP assets including material of differing levels of sensitivity.

4.2 This policy provides a high-level organisational objective for DWP with regards to Physical Security, but it is supported by MANDATORY Security Standards and Security Instructions which MUST be followed to ensure compliance, as they represent the minimum measures required to protect the security of DWP assets, information and people.

4.3 This policy is also supported by several useful guidance products which will assist the policy audience with implementation.

**Responsibilities**

5.1 All DWP employees, contractors, partners, service providers and employees of other organisations who are on DWP premises remain accountable for the security, health and safety of themselves, colleagues and the protection of Departmental assets including information and personnel.

5.2 The most senior grade based at each site, or in Moderate Risk and larger sites the Senior Responsible Officer (SRO), has responsibility for ensuring regular physical security risk assessments are conducted annually. They MUST ensure the action plans created to address identified risks and instigate business continuity activities are up-to-date, clearly communicated, regularly rehearsed, implemented effectively and readily available in accordance with their significance/importance/classification.

5.3 Except in a very small number of locations, managing the physical security controls of sites across the DWP estate is the responsibility of a contracted provider.

**Policy Statements**

6.1 Physical Security controls MUST be implemented that are proportionate to the risk appetite of the DWP and in adherence with the Information Security Policy and Acceptable Use Policy and other appropriate personnel and information security standards, including successful completion of Baseline Personnel Security Standard. This will support all staff to ensure they remain observant, report suspicious behaviour and highlight non-compliance. This vigilance will deter, delay, prevent and/or detect unauthorised access to, or attack on, a location and mitigate the impact should they occur.

6.2 Each DWP location presents unique physical security challenges and the measures introduced to protect each site must take into account the Risk Categorisation and the physical composition of that site. Effective approaches to Physical Security MUST follow the MANDATORY Security Standards and Instructions.

6.3 The most senior grade manager, or SRO in Moderate Risk and larger locations, MUST ensure that their site adheres to the Response Level Policy and ensure physical security risk assessment activity is conducted annually and that the action plans created to address identified risks are implemented.

**Compliance**

7.1 The level of risk and potential impact to DWP Information, assets and people will determine the controls to be applied and the degree of assurance required. DWP must ensure a baseline of physical security measures are in place at each site, and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required i.e. in response to a threat incident or change in the Government Response Level.

7.2 The implementation of all security measures must be able to provide evidence that the selection was been made in accordance with appropriate information security standards ISO27001/27002 and relevant HMG Policies and Standards.

7.3 The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated in order to meet new threats and other emerging vulnerabilities. Therefore, this policy and subsequent supporting guidance and standards will be subject to continual review and update.

**Appendix E - Acceptable Use Policy**

**DWP ACCEPTABLE USE POLICY**

**Contents**



## 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 DWP and fellow employees, suppliers, partners, citizens.

1.3 Use information, systems and equipment in line with DWP security and records management policies.

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 temporarily leaving 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 Only access citizen data where there is a valid business need that is appropriate to your job role.

3.2 Not save personal data into any document, spread sheet or system other than those approved by DWP Security for that purpose or which form part of approved local business processes aligned to security policy.

3.3 Ensure that data and assets exchanged with third parties (when appropriate) are protected by complying with the correct procedures and approvals process.

3.4 Not cause the unauthorised disclosure of citizen or staff or other sensitive 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

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.
- 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

**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 the Security Advice Centre with requests to unblock sites and not attempt to bypass DWP web filters.

6.4 Use social media appropriately by making themselves aware of the Cabinet Office guidelines and DWP guidance on social media / social media blueprint including DWP and Civil Service Values

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**

It is a Government and legal responsibility for DWP to act as a custodian of large amounts of sensitive and personal data, and to have the capability to monitor, manage and audit that information. For that reason we need to conduct DWP business on DWP equipment. There are also risks to individuals and DWP from use of personal devices for work purposes. We recognise that there may some limited circumstances where use of personal equipment for work purposes may be acceptable.

**Users will:**

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 USBs, when undertaking official business, unless working via encrypted links e.g. from home or hotels WIFI etc.

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

7.4 Not use any personal wallpapers or screensavers.

7.5 Raise software approvals or exception requests through the Security Advice Centre, considering risk against business delivery.

## 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. All exceptions to this policy must be submitted through 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.

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.