DWP Email Policy

Overview

The DWP Email Policy sets out responsibilities when using email to communicate with external organisations, citizens and between DWP email accounts.

The inappropriate use of email can pose many legal, privacy and security risks to DWP. Individuals must understand and comply with the requirements set out in this policy to manage the risks associated with the use of email.

The Email Policy and supporting **Checklist** detail what information can be sent via email to both DWP and non-DWP email addresses and under which circumstances.

Scope

The DWP Email Policy outlines the appropriate use of email by authorised persons and applies to all DWP employees and its representatives including contractors and suppliers, referred to in this document as “users”.

This policy applies to electronic communications of OFFICIAL or OFFICIAL-SENSITIVE information to overseas organisations as well as those in the UK.

This policy also applies to direct communications with individual members of the public and their legally appointed representatives. Section 6 of this policy does not apply to communications about Freedom of Information requests or where reasonable adjustments have been agreed to support individual citizens.

Email communications sent by accredited Trade Union Representatives concerning individual union member cases may be sent at the union’s own risk and are not covered by this policy.

The restrictions set out in paragraphs 1.9 - 2.3 of this policy do not apply when corresponding with:

- Members of Parliament (MPs) including Welsh Assembly Members and Members of the Scottish Parliament where the MP has requested a response by email.
- Complaints handled by the Independent Case Examiner where the MP or complainant has requested a response by email.
- Individual citizens who require **Reasonable Adjustments** under the Equality Act 2010 where DWP has agreed to support the individual’s communication needs in relation to a disability. Please refer to the **DWP Reasonable Adjustments Guide**.

Definitions

Information Classification is a process in which an organisation assesses the data that they hold and the level of protection it should be given. The **DWP Security Classification Policy** outlines the principles which DWP will apply to the classification and handling of its data using the baselines set by the wider HMG

Government Security Classifications (GSC) Policy. This Email Policy relates to information classified at OFFICIAL and OFFICIAL information marked with a SENSITIVE label.

Personal data is any information which relates to a living individual who can be identified from it, or who can be identified when that data is combined with other information. **Personal data** includes, but is not limited to names, identification numbers, dates of birth, residential or email addresses, information on family members, pensions, and health/medical information.

In DWP, certain types of personal data can be processed as OFFICIAL when transmitted by email. Please refer to the **Email Policy – Checklist** for emailing OFFICIAL personal data.

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

1. Policy Statements

1.1. Users of DWP email must ensure that they protect data in accordance with the **DWP Security Classification Policy**.

1.2. Users must comply with the **DWP Information Management Policy** in the creation, storage, and disposal of information shared and received through email.

1.3. OFFICIAL and OFFICIAL–SENSITIVE information may be sent to email addresses with a **gov.uk** suffix in addition to other **Trusted Partners**, subject to the restrictions detailed within this policy.

1.4. Users must ensure they understand and comply with the **DWP Offshoring of Information Assets Classified at OFFICIAL Policy** when making arrangements to exchange data with overseas organisations.

1.5. All users based in Wales must have a bilingual email signature and ‘Out-of-Office’ message. Users must also have a Welsh language disclaimer because the

automatic system sent disclaimer is in English. Please contact the **Welsh Language Unit** for help with this, including translation.

1.6 Users must ensure a brief and descriptive subject line is present on every email. Subject lines must not include citizen's personal data such as names, National Insurance numbers, dates of birth, and residential addresses.

1.7 Distribution lists that contain the email addresses of multiple recipients (including citizens) must only be created where there is a justifiable business reason to do so. These lists must be reviewed regularly to ensure currency. Access to these lists should be limited to users who have an existing business requirement.

1.8 When sending an email to multiple external recipients, users must consider whether it is appropriate to place email addresses into the visible fields ("To or Cc") or protect the identities of recipients by using the "Bcc" field or mail merge. Identities of citizens must always be protected from compromise. Please refer to the **Guidance on sending email to multiple recipients** for further information.

Emailing OFFICIAL information

1.9. Information classified OFFICIAL can be emailed to third party organisations provided that:

- The organisation has a legitimate business need to receive such information.
- The organisation is willing to receive the information by unencrypted email.
- The contents of the email or any attachments are not classified as OFFICIAL-SENSITIVE. If they are, the email **must be encrypted.**
- The email does not contain data exceeding the limits stipulated in the **Email Policy – Checklist.**

1.10 In relation to emailing single citizen records or multiple citizens records classified as OFFICIAL, users must consult the **Email Policy – Checklist**.

1.11. The **Email Policy - Checklist** applies to all OFFICIAL emails sent without encryption to organisations without the **gov.uk** email suffix and third-party partners/ suppliers which are not on the **Trusted Partners List**.

Emailing OFFICIAL-SENSITIVE information

1.12. Information classified OFFICIAL-SENSITIVE must be subject to additional controls to protect personal data and sensitive information as defined in DWP internal policies and processes. OFFICIAL-SENSITIVE data must only be shared via email when necessary or essential due to the risks associated with email.

1.13. Collating OFFICIAL data can increase the sensitivity of the overall dataset to OFFICIAL-SENSITIVE (see the **DWP Security Classification Policy** for more information). When sending collated data, users must refer to the **Email Policy – Checklist** to ensure that the amount of information being shared by email is appropriate.

1.14. Users must follow the **Data Transfer Procedures** when planning to share OFFICIAL-SENSITIVE data with third party organizations via email. Third party organisations include government organisations with the **gov.uk** email suffix, organisations on the **Trusted Partners List**, and all other third-party organisations. Information classified OFFICIAL-SENSITIVE must always be **encrypted** when sent outside the Trusted Partners List.

1.15. When sending information classified OFFICIAL-SENSITIVE to an internal DWP or other government department email address, users must include “OFFICIAL-SENSITIVE” in the email subject line.

1.16. Credit and Debit Card details such as card numbers and 3-digit card security codes must never be sent by email, including to colleagues using a DWP email address.

2. Arrangements with third-party organisations

2.1. When setting up new arrangements or projects with external organisations which involve sharing personal data (regardless of the classification level), users must consider if they need to follow the **Data Protection Impact Assessment (DPIA)** process. Users must also consider whether the arrangements should be documented on a **Data Sharing Agreement or contract**.

2.2. Communication with Third Party Contracted Suppliers via email, must always be subject to the terms and requirements of their contract.

2.3. Where it has previously been agreed that regular communications with a third-party organisation must be via more secure channels, such as secure or encrypted email, or email via other trusted networks, then these methods must always be used.

3. EMAILBLOCK

3.1. Users across all business areas in DWP should include **“E_M_A_I_L_B_L_O_C_K”** in their **email signature**. This offers protection against data breaches caused by accidental release of personal or sensitive information outside of DWP’s trusted networks. Please read the **E_M_A_I_L_B_L_O_C_K frequently asked questions** for more information.

3.2. Emails containing “E_M_A_I_L_B_L_O_C_K” will be blocked from leaving the DWP network if the receiving organisation is not on the Trusted Partner List. If an email needs to be sent outside of the Trusted Partners List and users have checked there is no OFFICIAL-SENSITIVE information contained within the email chain or any attachments, then “E_M_A_I_L_B_L_O_C_K” can be removed.

4. Acceptable use of DWP email

4.1. Users must only use appropriate and professional language in emails. Threatening, derogatory, abusive, indecent, obscene, racist, sexist, or otherwise offensive content must not be used and will not be tolerated.

4.2. Users must not engage in mass transmission of unsolicited emails (spam).

4.3. Users must not alter the content of a third party's email message when forwarding it unless authorised to do so.

4.4. Individuals must not assume the identity of another user or create/send material designed to mislead people about who originated or authorised it (e.g., through misuse of scanned signatures).

4.5. DWP email addresses must only be used for DWP business related activities and linked organisational activity (e.g., DWP discount schemes, Civil Service Learning, Civil Service Jobs, and HASSRA).

4.6. Users must not use their DWP email address to register for, or access, external websites for personal use. If a DWP email address has already been used to register for personal use (e.g., for retail shopping or internet banking purposes, etc) this must be changed to a personal email address as soon as possible.

4.7. Users must not use their home or personal email address to conduct any DWP official business. Users may, however, email their own personal details (e.g., their own CV, self-assessments, job applications and appraisal reports) to their home or personal email address. This is at the individual's own risk and in their own time, in line with the **Acceptable Use Policy**.

4.8. Any information emailed to an employee's home or personal email address must not include sensitive information such as details of DWP internal processes or personal data relating to any other individual (including colleagues or citizens).

5. Opening emails and attachments

Phishing is a technique used to acquire sensitive data (personal or business-related data), through fraudulent solicitation in emails or on a website, in which the perpetrator masquerades as a legitimate business or reputable person. DWP sometimes receives fraudulent emails and phishing attacks, so caution should be used when opening emails in personal and shared mailboxes.

5.1. Users must not open file attachments or links from suspicious sources and should be especially cautious where the origin is unknown and unsolicited.

5.2. All suspicious emails received must be reported to the **Security Advice Centre (SAC)**. Please refer to guidance on **How to Report Phishing Emails.**

Email mailbox management

5.3. Individual and shared email mailboxes must not be used as an archive or store for non-active team emails or employee/customer personal data.

5.4. Individual and shared email mailboxes must be regularly cleansed, and information moved to the appropriate storage, dependent on the classification as set out in the **DWP Information Management Policy**.

6. Email communications with citizens

6.1. If a customer provides their email address, DWP will assume that the individual is content for DWP to contact them by email. Before communicating with customers

via email, employees must explain DWP's limitations on the use of email, and how emailing personal data puts that data at risk of loss or theft. The limitations and risks of email must be discussed during the initial stage of the Customer Journey to manage and create the right expectations.

6.2. Emails to citizens and their legally appointed representatives must not contain OFFICIAL-SENSITIVE information but may be used to communicate generic, routine business information and data permitted by the **Email Policy - Checklist.**

6.3. Users must use a shared email address when contacting citizens as this helps protect employee identities and minimizes the risk of potential online abuse.

6.4. Requests must not be made of citizens for usernames, passwords, personal, health/medical or bank account information via email. DWP emails to citizens must contain **appropriate disclaimers** to communicate this.

6.5. Any unsolicited emails containing personal data received from customers, claimants, or clients must only be accepted if both the sender and message are validated using a known contact point (i.e., telephone or postal address) before the information is accepted as genuine and processed.

6.6. The Department allows the use of attachments and links in emails. However, the following must be adhered to when including links or attachments in emails to citizens:

- Attachments on emails to citizens must only be included where the citizen has requested the information or has been informed in advance to expect it.
- Links and attachments must only be used when they are completely necessary to deliver the business requirement.
- Users must avoid sending concealed links when directing a citizen to a website. The full URL must be provided.
- Wherever possible, business areas should seek to place blank forms and templates on GOV.UK and direct citizens to the website rather than using email to send individual copies to them.

Additional information on how to structure emails to citizens can be found in the **Service Manual - Planning and Writing Text Messages and Emails (link is external)(link is external)**.

7. Responsibilities

7.1. The Chief Security Officer (CSO) is responsible for the safety and security of DWP data, personnel, and assets. The CSO is responsible for reducing risk to the Department by overseeing the development, implementation, and maintenance of all security policies.

7.2. The Security Policy Team is responsible for the development, maintenance, and accuracy of security controls within the Email Policy

7.3. Line managers must ensure that their employees are aware of their responsibilities regarding the use of email as stated within this policy and ensure that their staff undertake the necessary training and understand the security requirements related to their role, including the potential consequences (criminal or disciplinary) that may result from inappropriate use.

7.4. All users have a critical role in protecting and maintaining DWP's information systems and data. It is the responsibility of all individuals to comply with the policies, procedures, and guidelines related to the protection of DWP information assets and systems.

8. Compliance

8.1. All DWP employees whether permanent or temporary, including DWP's contractors, have security responsibilities and must be aware of and comply with DWPs security policies and standards. Many of DWP's employees and contractors handle sensitive information daily and most security incidents and breaches relate to information security.

8.2. Compliance with this Email Policy is mandatory for all DWP employees and its representatives including contractors and suppliers. Users are responsible for understanding their responsibilities and the consequence of non-compliance as defined in this policy, the **Civil Service Code** the **DWP Acceptable Use Policy**, **DWP Information Management Policy** and **DWP Standards of Behaviour**.

8.3. Information security is important. In the most severe circumstances, non-compliance to policy may lead to dismissal. All security breaches **must be reported** to the Security Advise Centre. Not reporting a breach, or suspected breach, is a disciplinary matter.

8.4. 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.

8.5. If for any reason users are unable to comply with this policy, or require use of technology outside of its scope, they must discuss this with their line manager in the first instance and then the **Security Advice Centre** who can provide advice on escalation/exception routes.

8.6. An **exception to policy** may be requested in instances where a business case is made to undertake an exceptional activity which is not permitted normally and is non-compliant with DWP's Security Policies. This helps to reduce the risk of non-compliant activity and prevent potential security incidents.