DWP Email Policy

Contents

Introduction

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

Scope

The DWP Email Policy applies to all DWP employees and its representatives including contractors and suppliers.

Purpose

This policy aims to help users understand what information can be sent using email to both DWP and non-DWP email addresses and under what circumstances.

1. Emailing OFFICIAL and OFFICIAL-SENSITIVE information

1.1 In line with the DWP Security Classification Policy, OFFICIAL and OFFICIAL–SENSITIVE information may be sent to all email addresses with a gov.uk suffix in addition to other Trusted Partners, subject to the restrictions detailed within this policy.

Emailing OFFICIAL information

1.2 Information classified as OFFICIAL can be emailed to third party organisations that are not on the Trusted Partner list provided that:

- The organisation has a legitimate business need to receive such information.
- The organisation is content 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 needs to be encrypted.

- In the case of a prospective employer, no more than 10 CVs can be attached to the email or be contained within the body of an email.

1.3 In relation to sending individual records, employees must consult the Email Policy - Checklist

1.4 In relation to multiple citizen or employee data it is permitted to send the following details to non-Trusted Partner organisations without additional encryption:

- Names (including forenames/initials and surnames)
- National Insurance Numbers (NINOs)
- Reference numbers
- Additional details such as date of interview\appointment may be included if necessary

In emails to non-Trusted Partner organisations, there must be **no reference to:**

- Benefit payment amounts
- Child Maintenance payments or deduction amounts*
- Any additional personal details such as date of birth or home addresses, home or mobile telephone numbers or other contact details

*Please note – DWP can receive lists of Absent Parents NINOs and details of associated Child Maintenance payment or deduction amounts from employers – as stated above, additional personal identifiable information must not be requested.

1.5 This policy applies to transfers of OFFICIAL or OFFICIAL-SENSITIVE data to overseas organisations as well as those in the UK. Employees must ensure they are compliant with the DWP Offshoring of Information Assets Classified at OFFICIAL Policy when contacting organisations from overseas.

1.6 Employees must treat any email that contains data exceeding 500 OFFICIAL records, as OFFICIAL-SENSITIVE. Paragraphs 1.7 – 1.13 apply.

Emailing OFFICIAL-SENSITIVE information

1.7 Information classified as OFFICIAL-SENSITIVE must always be encrypted when sent outside of the Trusted Partners List.

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

1.9 Details of citizen’s financial information require a high duty of care when handling. Caution and careful judgement must be taken when handling financial information as there is a risk that citizens could be a victim of fraudulent or criminal activity.

1.10 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.

Arrangements with third party organisations

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

1.12 When emailing personal data (regardless of the classification level), employees must consider if they need to follow the Data Protection Impact Assessment (DPIA) process when setting up new arrangements with external organisations.

1.13 When making arrangements to share personal data on a regular basis, employees must consider whether the arrangements should be documented on a Data Sharing Agreement or contract.

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

1.15 The restrictions set out above do not apply to the requirements when corresponding with:

- Members of Parliament (MPs) including; Welsh Assembly Members, Members of the Scottish Parliament and members of the European 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.
- Where Reasonable Adjustments under the Equality Act 2010 have been agreed to support individual citizens with a disability, please refer to the list of DWP Reasonable Adjustments guidance.

2. Personal use of DWP email

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

2.2 DWP employees 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 or internet banking purposes) this must be changed to a personal email address as soon as possible.

2.3 DWP employees may email their own personal data (e.g. their own CV, self-assessments, job applications, appraisal reports, etc.) 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.

2.4 Any information emailed to employee's personal email accounts must not include personal data relating to any other individual (including colleagues or citizens).

2.5 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.

3. Email communications with citizens

3.1 This section of the policy relates only to direct communications with individual members of the public and their legally appointed representatives. It does not apply to communications about Freedom of Information requests or where reasonable adjustments have been agreed to support individual citizens.

3.2 If the claimant provides their contact details we will assume that the individual is content for DWP to contact them by email. DWP's limitations on use of email must be discussed during the initial stage of the Customer Journey to manage and create the right expectations by raising awareness of the risks of using email.

3.3 Email must not be used to send personal information to citizens. This includes date of birth, bank account details, information on family members, pensions and health/medical information. This excludes the minimum amount of contact information without which the communication would not be possible.

3.4 Email can be used to communicate generic, routine business information to citizens providing it does not contain personal data or any other OFFICIAL-SENSITIVE information. For other authorised exchanges see the list of circumstances which have been approved.

3.5 Wherever possible, employees must use a shared email address when contacting citizens as this helps protect employee identities and minimizes the risk of potential online abuse.

3.6 The Department allows the use of attachments and links provided that:

- 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
- Wherever possible, employees must avoid sending concealed links. When directing a citizen to a website, the full URL should be provided.
- Wherever possible, business areas must 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.

3.7 All emails to claimants and citizens must contain appropriate disclaimers which make it clear that DWP will never ask citizens for usernames, passwords, personal, health/medical or bank account information via email.

3.8 Email must be used as a reasonable adjustment where it is requested by an individual disabled citizen to support their additional communication needs. To read more about when a reasonable adjustment should be applied please see the operational instructions. Requesting communications via email must be for a valid reason which relates to the individual's disability.

3.9 To comply with the DWP Welsh Language Scheme commitment for external correspondence, all employees based in Wales must have a bilingual email signature and 'Out-of-Office' message. Employees 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.

3.10 Where unsolicited personal information is received from citizens and it is possible to process the information, both the sender contact details and message must be confirmed using a validated contact point before the information is accepted and processed.

3.11 Any business requirement that is not consistent with this policy must be raised with the Security Advice Centre (SAC) in the first instance and consideration should be given to the Security Policy Exception process if necessary.

4. Emailblock

4.1 It is compulsory for employees across all operational business areas in DWP to include "E_M_A_I_L_B_L_O_C_K" in their email signature. Other areas of the business should also consider using "E_M_A_I_L_B_L_O_C_K" to help protect DWP information.

4.2 Employees outside of operational business areas who do not include "E_M_A_I_L_B_L_O_C_K" in their email signature, do so at their own risk and may be subject to disciplinary procedures if there is a data breach.

4.3 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 a Trusted Partner. If an email needs to be sent outside of the Trusted Partners List and employees 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. Please read our E_M_A_I_L_B_L_O_C_K frequently asked questions for more information.

5. Compliance

5.1 Compliance with this Email Policy is mandatory for all DWP employees, contractors and anyone else using a DWP email account. 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 and DWP Standards of Behaviour.

5.2 DWP actively monitors employee and contractors use of internal IT and equipment to ensure everyone is complying with this Email Policy. Monitoring complies with and respects the privacy rights of all employees as outlined in the DWP Employee Privacy Notice.

5.3 It is a line manager’s responsibility to take appropriate action if individual users fail to comply with this policy. Please see the DWP Discipline Policy and the “How to: Deal with breaches of information security” guide.

5.4 The consequences of failing to comply with the Email Policy are serious and may attract disciplinary penalties up to and including dismissal.