Chapter 8: Information Security

Contents

Introduction

1. This guidance should be read in conjunction with the relevant provision specific guidance and your contract. It is provided as generic guidance for all providers delivering national employment programmes on behalf of Department for Work and Pensions (DWP).

2. Your DWP contract will detail what security policies and standards you must be compliant with. The DWP Security Policies and Standards can be found on the GOV.UK website.

Right of Access Requests

3. Right of Access requests replaced what was previously known as Subject Access Requests following the introduction of General Data Protection Regulation 25 May 2018.

4. Where possible claimants should be directed to the Right of Access online form which is submitted directly to DWP.

5. If you receive a Right of Access request from a claimant or participant solicitor or third party you must forward immediately to the Right of Access Gateway Team at rightofaccess.requests@dwp.gov.uk. The Gateway Team has 30 days in which to respond to the Right of Access request and communicate this to you.

Security Incident Reporting

6. You must comply with the DWP Security Standard SS-014 Security Incident Management.

Changes that Impact Compliance with DWP Security Standards and Policies

7. When requesting any change, modification or refinement to **any aspect** of your security plan or IT system that impacts on your compliance with DWP Security Standards and Policies you are required to submit a change request to DWP.

8. Completed change request documents should be sent to wpd.security@dwp.gov.uk. You should supply as much information about the proposed change as possible such as what contracts are impacted, architecture diagrams, data in scope, access levels, storage, support arrangements, offshore elements, audit and testing etc and include the name and contact details of the individual within your organisation leading on the change.

9. You must state whether your change is compliant with the DWP Security Standards and Policies and provide detail where the change is not compliant including any mitigating security controls.

Sharing Information

10. You may only share information in line with your DWP contract, DWP Information Management Policy and DWP Information Security Policy.

11. You **must follow** processes and procedures that you have agreed with DWP when returning data to DWP (including Jobcentre Plus).

Email Security

12. When sending DWP data by email you must first ensure that the recipient is entitled to receive that data and has a legitimate business need.

13. The sender is responsible for ensuring the safe transmission of DWP data ensuring all relevant standards are adhered to at all times.

14. You should only send the minimum amount of data needed to make the communication effective.

15. Wherever possible, Providers must use a shared email address when contacting citizens as this helps protect employee identities and minimizes the risk of potential online abuse. Individual DWP email addresses should not be included in such communications, only authorised DWP shared addresses where relevant.

Claimant CV and Name Unencrypted Email Exemptions

16. The following claimant or participant CV and claimant or participant name unencrypted email standards apply to **all provisions.**

Claimant or Participant CV Exemption

17. The unencrypted emailing of a claimant or participant's CV to their email account. The following conditions must be adhered to:
    - Only one CV to be sent per email,
    - The individual must have requested their CV to be emailed to them - CVs must not be emailed without the individual's prior consent - i.e. they must not be sent unsolicited,
    - A confirmation will need to be kept that the individual is content for their CV to be sent by email to their stated email address,
    - The following **must not** be included: date of birth, NINO, bank details, medical information, ethnicity and criminal record information.

Claimant or Participant Name Exemption

18. The unencrypted emailing of a full claimant or participant name to an employer or within your supply chain or to DWP provided the following conditions are adhered to:
    - Only one claimant or participant name per email,
    - Claimant or participant name only,
    - If any other identifiable claimant data is included within the email or subject line then encryption **must** be applied unless you have specific written permission from DWP to the contrary,
    - Confirm who the email recipient will be and that the email is received.

Supply Chain and Third Party Unencrypted Email Exemptions

19. Provider, subcontractor and service delivery partner staff are permitted to send an unencrypted e-mail within their supply chain or to a third party containing information about individual data subjects for the following situations:
    - up to 10 CV's,
    - up to 10 application forms,
    - up to 10 letters and
    - lists of claimant or participant names (up to 500)

    For emailing of DMA, Exit Reports, Change of Circumstances and Benefits Cap Notification please refer to provision specific guidance.

20. You must ensure you continue to adhere to the security requirements in your contract and associated guidance; if a Security Plan Change Request is required please follow the change process detailed in this chapter.

Emailing up to 10 CV's

21. You may send up to a maximum of 10 CV's by unencrypted email. This may comprise of CVs and or information directly extracted from a CV (single data set) but must not exceed the 10 CV/data set limit in a single email.

Emailing up to 10 Application Forms

22. You may send up to 10 application forms in one unencrypted email; for example, to a prospective employer.

23. Application forms must contain the minimum information to make the communication effective. You must not include NINOs, bank details or date of birth however the age of the claimant or participant may be included where appropriate.

24. Where application forms are for couples (each form includes data about two persons) then you must limit the number of forms to 5 applications per email to ensure each email contains information on no more than 10 claimants or participants in total.

Emailing up to 10 of the following types of letters

- Interview Letters,
- Job Offer letters,
- Appointment Letters.

25. No other letters are permitted to be sent by unencrypted email and using unencrypted email to send letters containing significant sensitive personal data is not permitted.

26. Limited personal data can be included to make routine communications effective however information about substance addiction or mental health issues for example **are not suitable** for transmission by unencrypted email.

27. NINOs and bank details must not be communicated by unencrypted email by yourself or your supply chain to employers for claimants or participants successful at interview.

28. Where there is a concern about the sensitivity of particular correspondence you should send it by more secure means such as encrypted email or by Royal Mail or a similar secure service.

Emailing Lists of Claimant or Participant Names (up to 500)

29. You may send a list of up to 500 claimant or participant names in 1 unencrypted email however you must always follow DWP guidance;

> "*In the case of a list of information about more than one data subject, and these are claimants: surnames and initials, or forenames, NINOs and/or reference numbers (additional simple details such as date of interview/appointment may be included if necessary) may be sent*".

30. There must be **no reference** to benefits payment amounts, child support payment amounts, or any additional personal details such as date of birth or home addresses, home or mobile telephone numbers or other contact details in these correspondences.

31. The **maximum** number of data subjects which may be included in a list in a single unencrypted e-mail is **500**. Any emails containing only a list of NINOs and no other information about the data subjects are not subject to this limit.

Claimant or Participant Data Not Permitted via Unencrypted Email

32. The following DWP claimant or participant data must **not** be included in unencrypted email when exchanging information with your **supply chain or third parties** unless you hold prior DWP approval to do so;
    - Date of birth,
    - Bank account details,
    - Medical history/mental health issues,
    - Substance abuse,
    - Criminal records,
    - Benefit payment details,
    - Children's names and dates of birth/age,
    - Ethnicity,
    - Sexual orientation.

National Insurance Number

33. NINOs must not be communicated by unencrypted email unless otherwise specified in the above exemptions or you hold prior DWP approval to do so.

Unencrypted Emailing of Data to DWP

34. You are permitted to use unencrypted email when sharing the following data with DWP:
    - Submission of UCNEA1s,
    - Submission of European Social Fund and European Social Fund (ESF) Match Funded Provision Good News Stories.

35. When emailing any of the above you must only attach one UCNEA1 or Good News Story per email.

36. The Supply Chain and Third Party Unencrypted Email Exemption - Emailing Lists of Claimant or Participant Names (up to 500) paras 28-30 of this guidance has been extended to permit you to use unencrypted email when sharing this data with DWP for ESF14-20, New Enterprise Allowance 2 (NEA2), Work and Health Programme (WHP), Intensive Personalised Employment Support (IPES) and Job Finding Support (JFS) England , Wales and Scotland. Please refer to provision specific guidance should a particular provision not be listed.

37. Please ensure you use clear and concise email header titles so it is clear to the recipient your emails intent.

Sending Clerical Information

38. Official and Official Sensitive documents may be posted using Royal Mail standard services although a fully tracked delivery service providing a signature as proof of delivery must be used for secure claimant items and sensitive data, e.g. medical records, certificates, identification documents.

39. You must not include a protective marking on the envelope.