

## Protocols for Handling Personal Data Securely

**These protocols are for everyone who has access to personal employee data. Personal data is data about living, identifiable individuals, including any opinions about an individual, whether held electronically or on hard copy documents.**

1. Like all employers, the DWP holds a range of data on its employees and this data is used for a number of legitimate reasons. However, access to this personal data can be open to abuse so we must be vigilant when dealing with the personal details of employees. HR practitioners, Employee Services (ES) employees, line managers and third party associates such as consultants/contractors) have a personal responsibility and a legal liability for ensuring the security of employee data.

2. This places an important responsibility on all of us who have access to personal employee data to ensure that:

- All personal employee data is treated confidentially i.e. is held securely and not divulged to anyone that does not have a legitimate business reason for seeing it
- Personal data is held only once on any data storage system and not duplicated
- Data that is held or processed should not be excessive in terms of the purpose for which it is being used.
- Access to employee personal data is restricted to those people who need it to carry out their job
- Appropriate [protective markings](#) are used for all documents containing personal employee data
- Personal data about employees must not be given to anyone who is not authorised to receive that data. When sharing personal data for legitimate reasons, it must be done in a secure way, e.g. via GSI email; internal departmental post systems; or secure fax i.e. where documents are collected at fax receiving end and not left unattended.
- Anyone who works off site should be particularly vigilant when using mobile phones and laptops in public places
- There are no DWP HR processes that require a combination of name, date of birth, and National Insurance number to be retained locally or processed together, and these details must never be recorded together on any DWP documents or local electronic systems
- New employees must have the required [background checks](#) (i.e. identity, nationality, and criminal record declaration) carried out before they start work in DWP

- Where paper records have been placed in confidential waste sacks, but not shredded, these sacks should be locked away (i.e. in a secure room or be in lockable confidential waste bin) until they can be safely disposed of

3. The security of documents containing personal data must be taken seriously and we must ensure that:

- Documents are securely held and kept in a locked drawer, cabinet or similar when not in use
- Keys for the locked cabinets are kept in a secure place with strict controls of access, e.g. where more than one person needs routine access a log to record access to the keys. Named line managers should be responsible for managing such controls, and checking that they are working adequately.
- Local clear desk policies are implemented and managers in HR and Businesses undertake periodic compliance checks
- Where documents/files containing personal data have to be removed from the office for legitimate reasons, this is recorded in a log or other record (this can be done on a bulk basis where appropriate). The method of recording and authorising will be decided at a local level.
- The security of any documents/files removed from the office for legitimate reasons is the responsibility of the person who logs them out
- Documents containing personal data should be destroyed as soon as they are no longer required and in line with the [Document Retention Schedule](#)

4. Personal information held on electronic systems (RM; Staff Information System; local databases and spreadsheets etc) can be particularly vulnerable so:

- All employees must adhere to the rules governing use of smart cards and not share personal passwords or personal access details
- Employee data which is held electronically must be password protected and access restricted appropriately
- Disks, CDs and flash-drives that are used to temporarily store employee data must be held safely and securely, i.e. in locked cabinets when not in use
- The movement of data should be by secure GSI email or carried on a guardian angel protected laptop but occasionally exceptions may occur. Where disks, CDs and flash-drives containing personal data have to be removed from the office for legitimate reasons, this is recorded in a log or other record. The method of recording will be decided at a local level. These disks and CDs should be destroyed, and the data on flash drives deleted, when the transfer /use of the data is finished.

- Employee records must not be processed on PCs or laptops, which are not the property of the DWP. Employees who use laptop computers for processing employee data must confirm that they have read and understood the [DWP Portable Computer Security Policy](#).
- Line managers and ES/HR staff who change roles and no longer need access to employee data for their job, must have their access to electronic systems altered accordingly and immediately

5. In exceptional circumstances employees may apply to have either or both their home address and telephone number removed from the RM system or to be set as an employee type 'protected'. The exceptional circumstances are:

- Where an employee's personal safety could be compromised if their details were made available. For example, if a Fraud Officer was dealing with a potentially violent person or an employee was involved in a domestic violence situation.

6. The procedure for an employee to obtain approval for extra security protection to be applied their RM record requires initial approval by their manager endorsed by a manager of SCS grade. The process is set out in the RM Tutor document 'Process for Protecting Records on RM'

7. Finally, if you have access to employees' personal data in your job, you are personally responsible for ensuring that it is kept secure and that it is only shared with those people who have authority to use it. Misuse of personal employee data or a failure to treat it securely is a disciplinary offence (on some occasions it may be a criminal offence under the Data Protection Act) and any breach of these protocols will be taken seriously.

8. More information can be found in the DWP [Security Policies](#), [Security Awareness E-learning](#), the [HR Data Handling Policy](#) and the [Document Retention Schedule](#).

9. Where you have any concern that a colleague is not complying with these procedures, you can raise the matter with your line manager, or if you prefer, with the Whistleblowers Hotline on 0800 9174881.