HSC Business Services Organisation

Movement and Transportation of Information Policy

Produced by the Human Resources and Corporate Services Directorate
Business Services Organisation
2 Franklin Street, Belfast, BT2 8DQ

Reference No:

Title:	Policy for the safeguarding, movement and transportation of records, files and other media		
Author(s):	Alan McCracken		
Ownership:	Director of Human Resources and Corporate Services		
Approval By:	BSO Board	Approval Date:	27/06/2019
Operational Date:	27/06/2019	Next Review:	27/06/2021
Version No.	2.0	Supersedes:	1.0
Key Words:	Data Protection, Information Security		
Director Responsible:	Director of Human Resources and Corporate Services		
Lead Author:	Alan McCracken		
Lead Author Position:	Data Protection Officer		
Additional Author(s):			
Department:	Corporate Services		
Contact Details:	dpa.bso@hscni.net		
Links to other Policies:	Information Governance Policy		
	Information Security Policy		
	Data Protection & Confidentiality Policy		

Contents

1. Introduction & Policy Statement

1.1 Everyone working for, with or on behalf of the Business Services Organisation (BSO) who records, handles, stores or otherwise comes across information has a personal common law duty of confidence to their employer.

1.2 Movement of records off-site may be required for a variety of reasons, including but not limited to the following:

- To facilitate meetings;
- To attend court;
- Recruitment, selection and other personnel management functions;
- To meet legal or statutory requirements, (such as audit functions or Directorate of Legal Services functions);
- For home working (where absolutely necessary).

1.3 This policy should be read in conjunction with the following specific BSO policies, as well as local procedures as necessary:

- Information Governance Policy
- Information Security Policy
- Data Protection & Confidentiality Policy
- Records Management Policy
- Policy for the reporting of Adverse Incidents, Accidents, Near Misses & Dangerous Occurrences

2. Purpose and Aims

2.1 The aim of this policy is to ensure that all staff safeguard all information they are in possession of while travelling from one facility/location to another during the course of their working day which includes traveling to or from home.

3. Scope

3.1 Confidential information may be contained in any portable media (whether paper or electronic), including but not restricted to work diaries, notebooks, case papers, client notes, HSC/external documents, portable computers, tablets etc.

3.2 This policy applies to **all staff**. In this document, the term ‘all staff’ refers to regular full-time, regular part-time, contractors, consultants, agency and temporary employees.

4. Responsibilities

4.1 The **Board** has overall responsibility to ensure compliance in all areas of information governance, including records management.

4.2 The **Chief Executive** and **Directors** have a duty to ensure that BSO complies with the requirements of legislation affecting management of the records and with supporting regulations and codes.

4.3 Managers are responsible for ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance with the standards set out in the documents that make up the Information Governance (IG) Framework.

4.4 Managers must also ensure that this policy and its supporting standards and guidelines are conveyed to their staff and any third party contractor working in the area, and ensure that staff are adequately trained.

4.5 Managers are also responsible for the establishment of an appropriate and effective system for tracking records within their area of responsibility.

4.6 All staff are responsible for:

- ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis;
- safeguarding any records / files / information that they remove from their central location;
- notifying their line manager immediately on suspicion of loss of any confidential information who will then initiate action in accordance with the "Policy for the reporting of Adverse Incidents, Accidents, Near Misses and Dangerous Occurrences" .

5. Tracking System

5.1 Effective systems must be in place for tracking the location of files containing confidential information, particularly when records are taken offsite. The type of system should be appropriate to the type of confidential information concerned (e.g. a card index system may be appropriate to a small department, while larger scale libraries may benefit from a computerised tracking system).

5.2 Detailed guidance on tracking/tracing systems should be documented in local departmental procedures and should take into account relevant professional standards where such exist. The following points should be incorporated:

- A clear record of the files which have been removed from the designated storage area, by whom and when, should be maintained;
- Files should be logged out to the relevant member of staff, who will be responsible for them whilst out of their designated storage area;
- The tracking/tracing system should be updated by the borrower if the files are passed on, prior to being returned to the storage area;
- Files should be returned as soon as possible and the register updated to reflect the return;
- A system for following up outstanding returns should be implemented.

6. Safeguarding of information transported between facilities / locations

6.1 It is recommended that employees should avoid taking confidential information outside the work base (e.g. to their home or to external premises) wherever possible. However, it is accepted that there are certain

circumstances where this will be necessary or unavoidable.

6.2 Departmental procedures should detail the level of authorisation required for the removal of files from BSO premises.

6.3 Confidentiality of the records is the sole responsibility of the staff member who has custody of them.

6.4 When confidential information is removed from BSO premises it is essential that its confidentiality and integrity is protected. The following guidelines should be followed:

- Keep the information in a secure container (e.g. sturdy case, or ziplock bag);
- Documents must be kept out of site and inaccessible to members of the public (this includes but is not restricted to staff, family members / visitors to your home) and not left unattended at any time (even for short periods) where they could be overlooked by any unauthorised person ;
- If materials are being transported by car they must be secured in the boot of the vehicle, locked and removed to a safer location at the first opportunity. Under no circumstances should materials be left in a car overnight;
- Hardware (laptops, etc.) must be kept securely;
- Staff should wherever possible transport information in digitally encrypted formats and devices;

6.5 Departmental procedures should detail any other specific requirements.

7. Non-Compliance

7.1 A failure to adhere to this policy and any associated procedures may result in disciplinary action.

7.2 Serious breaches may be reported to the PSNI, Information Commissioner's Office or other public authority for further investigation.

8. Review

8.1 This policy and any associated procedures will be reviewed no later than every 2 years, to ensure their continued relevance to the effective management of Information Governance within BSO.

9. Equality Statement

9.1 This policy has been screened for equality implications as required by Section 75 of Schedule 9 of the Northern Ireland Act and it was found that there were no negative impacts on any grouping. This policy will therefore not be subject to an Equality Impact assessment.

9.2 This Policy has been considered under the terms of the Human Rights Act 1998, and was deemed compatible with European Convention Rights contained in the Act