Business Services Organisation

POLICY FOR THE SAFEGUARDING, MOVEMENT & TRANSPORTATION OF RECORDS, FILES AND OTHER MEDIA

Reference No:	**BSO-CS 10**
Version:	**1**
Ratified by:	**BSO Board**
Date Ratified:	**30/04/2015**
Date Equality Screened:	**19/03/2015**
Name of Originator/Author	**Bill Harvey Amended HMCP following SMT meeting**
Date of Policy	**25/03/15**
Name of responsible committee/individual	**DHRCS**
Date Issued:	**13/05/15**
Policy Reviewed date:	**07/04/2017**
Next Target Review Date	**07/04/2019**
Target Audience:	**All BSO Staff**
Distributed Via:	**Intranet, Hard Copy**

Amended by:	
Date amendments approved:	

Table of Contents

1. INTRODUCTION

1.1 The aim of this policy is to ensure that all BSO staff/contractors 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. It should be read in conjunction with specific local departmental procedures as necessary.

1.2 This may include confidential information contained within work diaries, notebooks, case papers, client notes, HSC/external documents, portable computers, tablets etc.

1.3 It is the responsibility of all staff to familiarise themselves with the contents of this policy.

2. GUIDING PRINCIPLE

2.1 Everyone working for or with the BSO who records, handles, stores or otherwise comes across information has a personal common law duty of confidence to his or her employer. This applies equally to those, such as student placements, trainees, agency workers and those on fixed term contracts and where appropriate and possible external contractors.

2.2 Staff must notify 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 & Dangerous Occurrences."

2.3 Managers must ensure staff are aware that disciplinary action may be taken when it is evident that a breach in confidentiality or loss of information has occurred as a result of a member of staff's neglect in ensuring the safeguarding of confidential information.

3. TRACKING / TRACING RECORDS

3.1 Managers must ensure that effective systems are in place for tracking the location of files containing confidential information. 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. 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 into Departmental guidelines:

a) A clear record of the files which have been removed from the designated storage area, by whom and when, should be maintained;

b) Files should be logged out to the relevant member of staff , who will be responsible for them whilst out of their designated storage area;

I. The tracking/tracing system should be updated by the borrower if the files are passed on, prior to being returned to the storage area;

II. Files should be returned as soon as possible and the register updated to reflect the return;

III. A system for following up outstanding returns should be implemented;

IV. Responsibility for the establishment of an appropriate and effective system should be assigned to the IAO within the Department.

4. MOVEMENT OUTSIDE THE WORK BASE

4.1 Movement of records off-site may be required for a variety of reasons, e.g.

a) To facilitate meetings;

b) To attend court

c) Recruitment, selection and other personnel management functions;

d) To meet legal or statutory requirements, (such as audit functions or Directorate of Legal Services functions);

e) For home working (where absolutely necessary).

This list is not exhaustive.

5. RECORDS STORED OVERNIGHT IN THE EMPLOYEES HOME

5.1 In some circumstances, records may be kept at the staff member's home e.g. materials required for a court appearance, recruitment exercise etc. Confidentiality of the records in the staff member's home is the sole responsibility of that member and they should be made fully aware of this by their line manager.

6. SAFEGUARDING OF INFORMATION TRANSPORTED BETWEEN FACILITIES/LOCATIONS

6.1 It is recommended that employees should avoid taking confidential information outside the work base wherever possible. However, it is accepted that there are certain circumstances where this will be necessary or unavoidable. Departmental procedures should detail the level of authorisation required for the removal of files from BSO premises.

6.2 BSO employees physically collect and deposit files and/or documents and other information from clients as part of their function. It is essential that when said materials are removed from the BSO/Trust/External premises, personal/confidential information is kept securely and the following guidelines should be followed to ensure it is adequately protected:-

a) Keep the information in a secure container, for example, a sturdy case, or other suitable secure container;

b) Keep the information out of sight; 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. Any such materials should not be left in an unattended car. They must not under any circumstances be left in a car overnight.

c) All files in transport must be kept closed in order that contents are not seen accidentally;

d) Documents must be Inaccessible to members of the public and not left even for short periods where they might be overlooked by unauthorised persons including other staff;

e) Do not leave personal information unattended at any time;

f) If it is necessary to take personal information home, ensure that it is cannot be accessed by other family members or visitors;

g) Make sure laptops and other software are kept securely.

h) Departmental procedures should detail any other specific requirements.

i) Staff should wherever possible transport information in digitally encrypted formats and devices.

7. RELATED POLICIES

- Information Governance Policy
- Security Policy
- Data Protection & Confidentiality Policy
- Policy for the reporting of Adverse Incidents/Accidents/Near Misses & Dangerous Occurrences
- A Professional Approach to the Management of Security in the NHS.