



Business Services
Organisation

BSO CLEAR DESK AND SCREEN POLICY

(version 1.0)



Approved at BSO Board on 25th February 2010

CONTENT

1. PURPOSE	3
2. DATA CLASSIFICATION.....	3
3. THE DESK / OFFICE ENVIRONMENT	3
4. THE PC ENVIRONMENT	4
5. PRINTERS / FAXS / PHOTOCOPIERS	4
6. DISPOSAL PROCEDURES	5
7. MONITORING	5

1. PURPOSE

1.1 The BSO has adopted a clear desk policy for papers and removable media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorised access, loss of and damage to information during and outside normal working hours.

1.2 This policy applies to **all staff**, including regular full-time, regular part-time, contractors, consultants, agency and temporary employees.

1.3 Further information on record management is available from the BSO Record Management policy.

2. DATA CLASSIFICATION

2.1 All staff must be careful when handling any HSC information and especially when dealing with sensitive or personal data.

2.2 The *Code of Practice on Protecting the Confidentiality of Service User Information* document issued by DHSSPS in January 2009 provides guidance on the handling of personal information.

The document can be found on the DHSSPS web site

<http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf>

2.3 Examples of sensitive and personal information include but are not limited

to:-

- copies or extracts of data from clinical systems;
- commercially sensitive information;
- contracts under consideration;
- budgets;
- staff reports;
- appointments – actual or potential not yet announced;
- disciplinary or criminal investigations.

2.4 Personal data is further defined by the Data Protection Act (1998).

3. THE DESK / OFFICE ENVIRONMENT


3.1 The following controls should be followed:-


- Keep file cabinets and cupboards closed and locked and do not leave keys in their locks.
- Paper and computer media must be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours;

- Sensitive or critical business information must be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated;
- Desks and furniture should be positioned so that sensitive material is not visible from either the windows or the hallway. Closing blinds on windows may provide an alternative. This may be particular relevant where visually impaired members of staff use larger fonts and or Windows Accessibility functionality including the Magnifier.
- Where audio software is used e.g. Microsoft Narrator, the audio should be directed through headphones to prevent others from hearing potential sensitive information.
- Do not use bookshelves to store binders with sensitive information. Label those binders appropriately and lock them up.
- Arrange folders in file cabinets so that the least sensitive are in front, most sensitive in back.
- Erase whiteboards at the end of meetings.
- Do not leave any personal effects on show or unattended at anytime e.g. bank statements, letters. Key private information may be viewed by others.
- Keep mobile devices with you, and lock phones and PDAs with a pass code.
- Never leave your access cards or keys out anywhere; always keep them with you.
- Unclassified and non-sensitive material such as magazines and manuals may be placed on desk, bookcases etc. but must be stored in a tidy manner.
- Notify the HSC ICT Security Manager immediately if access cards or keys are missing.

4. THE PC ENVIRONMENT

4.1 The following controls should be followed:-

- Never write your passwords on a sticky note nor try to hide them anywhere in your office.
- Enable the password-protected screen saver (Windows Logo Key  +L) when you leave your desk.
- In a shared PC environment, close applications when you leave the PC.
- Do not leave portable media such as CDs or USB data pens in drives.
- Turn off your PC when you leave for extended periods.
- Consider using a screen filter to minimize the viewing angle on a computer monitor.

TIP – Use Windows Logo Key  +M to minimise all open applications on your PC to prevent unauthorised people from viewing sensitive data.

5. PRINTERS / FAXS / PHOTOCOPIERS

5.1 The following controls should be followed:-

- Sensitive information, when printed, should be picked up immediately.
- Photocopiers should be locked (or protected from unauthorised use in some other way) outside normal working hours;
- Incoming and outgoing mail points and unattended fax machines should be protected.

6. DISPOSAL PROCEDURES

6.1 The following controls should be followed:-

- Staff must continuously review any paper they hold and dispose of waste immediately.
- Where HSC information has been taken home in paper format always return it to the office for disposal.
- Never dispose of any HSC information via normal office cleaning services.
- Waste paper must not be allowed to build up in cupboards, drawers, bookcases, filing cabinets, desks, floor space, around printers or communal areas.
- Where information is extremely sensitive it should be shredded immediately using the office shredder.
- Separate sensitive information from the remainder of paper for disposal (Red bags) and store in a locked cabinet outside normal working hours. This paper is shredded before being removed from the premises by the approved supplier.
- Use the White bags to dispose of all other paper. This paper is compressed and baled and therefore not rendered unreadable.
- No bags should be allowed to become over full (i.e. cannot be comfortably and safely carried by one person) before sealing and removal to the nearest designated collection point.
- All removable media at the end of its life that contained HSC information must be returned to BSO-ITS for destruction.
- Further information is available from the BSO Record Management policy.

7. MONITORING

7.1 Compliance with this policy will be monitored regularly and reports passed to the appropriate management for consideration.