Security of Information Processing Equipment Policy

(formerly a guideline on the physical security of information processing equipment)

Approved by: Policy and Guideline Committee
Date Approved: 13th February 2007
Most Recent Review: October 2008
Next Review Date: September 2010

This policy is currently under review and should be continued to be used.
If any queries or concerns, please contact the Head of Privacy
Index

1. Introduction .................................................................................................3
2. Definition of Information Processing Equipment ....................................... 3
3. Physical Security Guidelines. ................................................................. 3
4. Category 1 – Desktop Devices ...................................................................3
5. Category 2 – Servers ..................................................................................4
6. Category 3 – Removable/portable media .................................................. 5
   6.1. Paper files ........................................................................................... 5
   6.2. Electronic media ................................................................................. 5
7. Category 4 – Medical/Laboratory Equipment ............................................ 7
8. Clear Desk/Screen ......................................................................................7
9. Disposal of Information Processing Equipment ......................................... 8
10. Compliance with this procedure .............................................................9

Change Control

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/2008</td>
<td>GL</td>
<td>• Change from guideline to procedure to reflect the necessity of compliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specific instruction on USB drives and other removable media. Include reference to e-learning training Section 6.2.</td>
</tr>
<tr>
<td>12/2007</td>
<td>GL</td>
<td>This document has been amended (Category 3 equipment) to reflect Connecting for Health Guidance issued in November 07.</td>
</tr>
<tr>
<td>2/2007</td>
<td>RM</td>
<td>Base document</td>
</tr>
</tbody>
</table>
1. Introduction

This document is intended to give provide staff with instruction on how to comply with the Information Security Policy (DMS No 12212) and the Data Protection Policy (DMS No 11800).

See also the Removal of Information from Trust Premises Policy (DMS No 33951)

2. Definition of Information Processing Equipment

Information Processing Equipment can be divided into 4 categories:-

1. Desktop Devices
2. Servers
3. Removable/Portable Media
4. Medical/Laboratory Equipment – This category constitutes all equipment, not included in the above categories, which is used within the Trust and which collects, stores, manipulates and/or produces information.

3. Physical Security Guidelines

General statement – The physical security afforded to any piece of information processing equipment must be commensurate with the operational requirements of the Trust, the value of the equipment and the nature of the information held on and/or processed by it. Where possible, all such equipment should be clearly marked as being the property of the University Hospitals of Leicester NHS Trust.

4. Category 1 – Desktop Devices

This category covers a large number of different devices including (the list is not exhaustive):

- PCs,
  - Laptops,
  - Printers,
- Thin Client devices,
- Scanners,
- Photocopiers,
- Projectors,
- Video/DVD Players/Recorders,
- TVs

It is accepted that, in order to provide healthcare services, the Trust's hospital sites are open to the public 24 hours a day 7 days a week and that, to be effective, equipment must be available and easily accessible by staff needing to use it. These requirements limit the level of security which can be applied to devices in areas which are open to the public.

In areas open to the public, devices should, where possible, be

- stored out of site
- “security” marked with the hospital details and
- attached, by means of a security cable or other such device, to an appropriate anchor point.

Staff working in such areas should be made aware of the equipment that is held there and should be instructed to challenge anyone they see tampering with or attempting to remove it. Commercially sensitive or personally identifiable information should not be stored on this equipment, either on hard disks (on PCs or laptops) or in memory (on PCs, laptops and some printers, scanners and photocopiers)

In areas not open to the public, similar security measures to those detailed above should be applied, where appropriate. These areas, however, are usually not constantly manned by Trust staff and it is therefore it is more important to apply normal office security measures such as always ensuring that doors are locked when the area is unmanned, that windows in ground floor offices are closed and, preferably, locked and that equipment is not easily seen from outside.

Printers, scanners and photocopiers which incorporate internal memory features should have these facilities disabled unless specifically required. If such facilities are used, care must be taken to clear the memory once documents held in it are no longer required. These devices should not be used as general document storage facilities.

Video/DVD players/recorders and TVs should be stored in locked cabinets where possible.

5. **Category 2 – Servers**

Separate guidance on the security of server rooms is published under the title Server Room Security which forms a part of the IM&T Risk Analysis Process.
6. Category 3 – Removable/portable media

This category covers a large range of methods of storage and manipulation of information; examples of which include (the list is not exhaustive):

- Floppy disks
- USB or Pen drives
- CDs and DVDs
- External hard drives
- Cameras
- PDAs
- Mobile telephones
- Paper files
- Dictaphone tapes

6.1. Paper files

The security surrounding all such media must be commensurate with the nature of the information held on it. In general, however, the following should be considered:

- When not in use, the documents should be kept locked away out of site
- In the case of paper records, extra copies should not be taken unless absolutely necessary and, if they are taken should be clearly marked as copies and destroyed at the earliest opportunity
- In cases where patient information is held and where practical, this should be anonymised.
- Paper records should not be left in places where they can be easily seen and read by unauthorised individuals.

6.2. Electronic media¹

Since UHL computers are all connected to a network which allows sharing of data within the Trust, the use of removable media such as memory sticks and CDs implies that information is going to leave UHL premises. This should be a rare occurrence so the use of removable media should be questioned. If there is a need to use removable media, the following must be adhered to:

- Any bulk extracts of confidential or sensitive data must be authorised by the responsible senior manager for the work area.

¹ Based on the DoH document - NHS Removable media - Information security template, 30/11/2007
University Hospitals of Leicester

- IT is responsible for identifying and implementing security arrangements on Trust computers in accordance with DoH advice and standards. The security arrangements must not be circumvented. Any queries on security arrangements should be directed towards the Help Desk (8000).

- USB/pen drives must be approved by IM&T. (This will be enforced technically in the near future).

- Floppy disks, CDs, DVDs and any other removable storage device which contains personal or confidential data must be encrypted to DoH standards.

- Line managers are responsible for:
  - the day to day management and oversight of removable media used within their work areas to ensure this policy is followed;
  - the secure storage of all unallocated removable media and its related control documentation as required by this procedure;
  - ensuring that staff involved in data extraction and data file creation are fully aware of Trust policies, procedures and guidelines. (Note, e-learning entitled Secure Transfers of Personal Data is available free of charge on Insite.)

- Staff who have been authorized to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as highlighted in these guidelines. Failure to comply with this removable media policy may endanger the information services of UHL and will be investigated under HR policies.

- Removable media may only be used to store and share NHS information that is required for a specific business purpose. When the business purpose has been satisfied, the contents of removable media must be removed from that media through a destruction method that makes recovery of the data impossible. Alternatively the removable media and its data should be destroyed and disposed of beyond its potential reuse. In all cases, a record of the action to remove data from or to destroy data should be recorded in an auditable log file;

- Removable media should not be taken or sent off-site unless a prior agreement or instruction exists. A record must be maintained of all removable media taken or sent off-site, or brought into or received by the organization. This record should also identify the data files involved;

- Removable media must be physically protected against their loss, damage, abuse or misuse when used, where stored and in transit;
• Data archives or back-ups taken and stored on removable media, either short-term or long-term, must take account of any manufacturer’s specification or guarantee and any limitations therein;

• All incidents involving the use of removable media must be reported to IT and through the Trust’s incident reporting mechanism.

7. Category 4 – Medical/Laboratory Equipment

This category constitutes all equipment, not included in the above categories, which is used within the Trust and which collects, stores, manipulates and/or produces information.

Users of such equipment must be aware that information stored within it may be of a sensitive nature. The following should therefore be considered when dealing with it:-

- When not in use, the equipment stored securely to prevent theft
- Information should not be held on the equipment for longer than is necessary.
- Staff using such equipment must not only be trained in its operation but also made aware of the information held on it to remove it (when no longer required).
- An understanding of the nature of information storage must form a part of the acceptance testing phase for any new equipment.

8. Clear Desk/Screen

Users should adopt a clear desk and clear screen policy to reduce the risks of unauthorised access, or accidental damage to or loss of sensitive or confidential information.

All sites shall adhere to a clear desk, clear screen policy in relation to confidential, patient-identifiable or other sensitive information. A clear desk, clear screen policy does not necessitate the removal of all paperwork from a desk or information from a screen, it does, however, involve the treatment of any information which could be regarded as confidential, patient-identifiable or sensitive in any other way.

The provision of healthcare often involves constant use of confidential information in areas open to the public where it is vulnerable to unauthorised access. In addition, visitors, some temporary and contract staff, security and cleaning staff, are examples of people with authorised access to secure, access controlled sites, who are not authorised to view confidential or
sensitive data. The nature of the data and not site location dictates how and when this policy is applied. Where confidential (patient identifiable) or other sensitive (e.g. employee’s pay scale) information is involved, users must, as and when appropriate:

- Remove all sensitive information from the workplace and lock away, in a drawer or preferably in a fire resistant safe or cabinet. This includes all patient identifiable information, as well as other sensitive (personal or business) information such as salaries and contracts.
- Store visit, appointment or message books in a locked area when not in use.
- Angle computer screens away from the view of patients and visitors.
- When leaving a workstation either log out or, in the case of a PC, lock the screen.
- Store paper and computer media in secure cabinets or safes.
- Locate photocopiers and printers so as to avoid unauthorised use.
- Ensure that post-it notes and sticky labels holding patient-identifiable or other sensitive information are not left to public view.
- Before a patient enters a consulting room, remove all evidence of the previous patient from view (computer screens, medical records, test papers or samples etc).
- Lock all consulting rooms and office areas when they are not in use.

Reception desks and Nurses Stations can be particularly vulnerable to visitors. These areas should be kept as clear as possible at all times, in particular medical records should not be left open and with other patient identifiable information, should not be held on the desk or within reach/sight of visitors or patients.

9. Disposal of Information Processing Equipment

Great care must be exercised when disposing of any equipment which has been used in the processing of information if there is any possibility that some information may remain in/on it.

In cases where the information is held electronically, reference must be made to IM&T for the appropriate action to be taken (Note – formatting a disk and/or overwriting a tape does not necessarily destroy the information held on it). IM&T will arrange for the physical destruction of the media.

The disposal of computing equipment is covered by the WEEE (Waste Electrical and Electronic Equipment) regulations and must therefore be done in an appropriate and legal manner.

In cases where information is held on hard copy (paper, film, etc.), when no longer required (see the Retention Policy) the media must be shredded.
10. Compliance with this procedure

Spot checks may be conducted to ensure this guideline is complied with. Any compliance issues will be investigated and reported to the line managers concerned.