Secure Storage, Disposal and Destruction of Electronic Equipment and Media Policy
Secure Storage, Disposal and Destruction of Electronic Equipment and Media Policy
– EXECUTIVE SUMMARY

<table>
<thead>
<tr>
<th>Key Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles of IT Hardware, removable media, secure storage, disposal and Destruction</td>
</tr>
<tr>
<td>• Understanding Obligations</td>
</tr>
<tr>
<td>• Confidentiality and Legal Compliance</td>
</tr>
<tr>
<td>• Information Security</td>
</tr>
<tr>
<td>• Quality Assurance</td>
</tr>
<tr>
<td>• Legal and Related Policies and Guidance</td>
</tr>
<tr>
<td>• Secure Storage, Disposal and Destruction</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Minimum Implementation Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Good Practice for Managers</strong></td>
</tr>
<tr>
<td>• Has identified the staff in his or her area to whom this policy applies and has given the policy (or selected excerpts) to them.</td>
</tr>
<tr>
<td>• Has assessed the impact of the policy on current working practices, and has an action plan to make all necessary changes to ensure that his or her area complies with the policy.</td>
</tr>
<tr>
<td>• Has set up systems to provide assurance to him or her that the policy is being implemented as intended in his or her area of responsibility.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Good Practice for Employees</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Has read the policy (or selected excerpts) and considered what it means for him or her, in terms of how to conduct his or her duties.</td>
</tr>
<tr>
<td>• Has completed any mandatory education or training that may be required as part of the implementation of the policy.</td>
</tr>
<tr>
<td>• Has altered working practices as expected by the policy.</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction and Scope
2. Asset Inventory
3. Storage
4. Transportation
5. Secure Disposal and Media Destruction
6. Electronic Storage Media

Appendix A – Secure and Confidential Data Destruction Service
1 Introduction and Scope

All electronic hardware or equipment and removable media should be managed and disposed of in a secure manner when no longer required. This is required to comply with the Data Protection Act 1998, and Information Commissioners’ Office guidance on “IT Disposal for organizations”.

- All departments must ensure responsibility for asset disposal is assigned to a named individual.
- A complete inventory of all equipment, including those classified for disposal must be available.
- All staff should be clear about what happens to devices that are not required.
- Methods of disposal must be risk assessed prior to use.
- “data processor” contracts must be in place with any external contractors to ensure appropriate security controls are in place.
- No device is permitted to be recycled without all personal data being securely deleted to a standard approved by eHealth.

Prior to disposing of any data or equipment, employees should consult the NHS Lothian Retention and Destruction of Records and Records Management Policies, to ensure that it is appropriate to dispose of the data. These policies outline the retention periods for information, and covers employee records, administrative records, estates records, reports, investigations and complaints etc.

All staff must ensure compliance with this policy. All employees will be informed of the appropriate methods of disposal of decommissioned or unwanted equipment, media or data through staff training, Policies and guidance.

NHS Lothian eHealth, and all other NHS Lothian departments will have local procedures to ensure implementation of this policy.
NHS Lothian eHealth will provide this service for all Assets purchased by the eHealth department. Departments with equipment not purchased by eHealth must ensure they have procedures to comply with eHealth policy, and these will require to be funded locally as appropriate.

eHealth Security Policy
NHS Lothian Records Management Policy : Retention and Destruction
NHS Lothian Data Protection Policy
2. Asset Inventory

Assets are defined as Devices with Storage media, including all IT devices hardware or equipment and removable media including hard drives. All assets must be tracked using an inventory management tool, from delivery, transport to user location and up to and including evidence of destruction. Other storage medias e.g. CD/DVD, NHS Lothian encrypted Memory Sticks, SIM / Memory Cards and Magnetic Tapes and Microfiche must be stored securely.

3. Secure Storage

When not in operational use, all assets must be securely stored. eHealth and local departments will risk assess each approved storage area. Assets in operational use must be subject to eHealth Security Policy.

4. Transportation

All equipment and assets taken away from Hospital premises must be transported in accordance with the following guidance for transportation of electronic equipment and removable media within NHS Lothian. This includes Hard Drives removed from Servers or PC’s, including the complete systems being transported. Policy for Transporting storage media that does not come under “removable media”, that may contain sensitive data or records and must comply with Safe Transfer of Records Policy.

Staff must use NHS Lothian vehicles. If personal vehicles are used this would require to be agreed in advance with line managers.

All staff must seriously consider the need for taking equipment out of their base with them on a visit. This should only happen when absolutely essential. Staff must not carry around more equipment than is necessary. It is recognised that staff may find it necessary to remove equipment from their base, to provide a service. The guidelines below should be followed to reduce the risk of the equipment being accessed by an unauthorised person, lost or stolen.

- When removing equipment or media staff must ensure that this is only equipment for those visits that are pre booked.
- Only the equipment or media required to carry out the visit should be transported.
- A record of equipment being transferred must be kept.
- Small Equipment should be store be stored and carried in a secure bag/case.
- If multiple equipment is required to be transported, this may if required be stored and locked out of view, i.e. in the car boot or rear section of a van for the minimum period required.
- If the member of staff is not returning to their base at the conclusion of their visits the equipment must be stored in the bag/case used and taken out of the car/van overnight into their home. Care must be taken in order that members of the family or visitors to the house cannot gain access to equipment. This practice should only occur if the member of staff is not returning to their base after the working day or the equipment is required for the next working day. Staff must have the prior written agreement of their manager if it is necessary for them to work in this way.
• Equipment should not be away from base for more than one working day i.e. if a member of staff is not returning to base at the conclusion of their working day, the equipment taken out on visits must be returned on their next normal working day, unless formal management agreement is provided for alternative arrangements.

There may be exceptional circumstances that mean this is not possible i.e. if a member of staff goes off sick before returning the equipment. In this situation equipment should be returned as soon as is practically possible. Managers may have to make arrangements to retrieve equipment whilst the member of staff is off for a period of time.

5. Secure Disposal and Media Destruction

All IT equipment or storage assets will be disposed to accredited companies Authorised suppliers as risk assessed by the Information Governance and Security team, and as appropriate Data Processing contracts put in place prior to commencement of service.

All storage media Hard Disk drives should be removed prior to disposal for safe destruction. If storage media cannot be removed a risk assessed approach must be agreed with eHealth to determine acceptable destruction or permanent data removal.

A record of all items destroyed must be kept including serial numbers if available and/or destruction certificates.

All NHS Lothian identifications must be removed from equipment prior to disposal.

All equipment must comply with electronic disposal guidelines (WEEE Waste Electrical and Electronic Equipment Regulations 2013).

6. Electronic Storage Media

Electronic storage media will include all of the items listed in the table below. This is not an exhaustive list of all possible media as technology will evolve and new media will become available as time progresses.

Below are the most common types of media in use at this time. This Policy will be updated regularly and therefore take account of new media throughout the review period, but there is individual responsibility for ensuring that all media is securely stored and disposed.

Media How to Dispose

eHealth will dispose of all eHealth assets and media, but it is the responsibility of non eHealth departments to manage and if required fund the process of disposal according to this policy. Instruction on approved disposal methods are listed below.

1. Devices with Storage Media

This includes but not limited to; Servers, PCs or Laptops, Mobile Devices/Tablets. Hard disks will be securely stored onsite and subsequently destroyed onsite to the
agreed standard by an eHealth authorised external contractor before issuing a destruction certificate and removal for recycling. If storage media cannot be removed a risk assessed approach must be agreed with eHealth to determine destruction or permanent data removal.

2. **CD/DVD**
Writeable or rewriteable CD/DVD must be shredded. This is acceptable to be performed internally if the correct equipment is available. Otherwise this must be by an eHealth authorised external contractor.

3. **NHS Lothian encrypted Memory Sticks**
Returned to eHealth. Must be destroyed. This must be by authorised external contractor.

4. **SIM / Memory Cards**
Returned to eHealth. Must be shredded. This must be an eHealth authorised external contractor.

5. **Magnetic Tapes and Microfiche**
Must be shredded. This must be by an eHealth authorised external contractor.
Appendix A : SECURE AND CONFIDENTIAL DATA DESTRUCTION SERVICE

A contract will be established that will meet all legal and regulatory requirements for secure confidential disposal of assets. Contracts will include the safe destruction and disposal of electronic storage devices and media.

A scheduled collection (for locations producing confidential waste on a regular basis) or a reasonably frequent ‘on-demand’ collection will be established.

Authorised Service Provider

A security risk assessment and audit will be performed by eHealth on companies that can conform with WEEE guidelines, before establishment of a data processing agreement permitting them to be contracted by NHS Lothain for disposal.

Contract Scope

There should also be provision under the contract for the secure destruction of CDs, DVDs and telephone SIM cards, the materials from which are also recycled.

Additionally, the supplier has provided evidence of a service capable of securely shredding audiotape, videotape, data tapes, and microfiche to appropriate industry standard for the content of the media.

Certificates of destruction recording the originating location and type of data destroyed to be provided to NHS Lothian prior to removal of equipment or media.