Information Security Policy
Secure Use of Removable Storage Devices

<table>
<thead>
<tr>
<th>Author:</th>
<th>Information Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Lead Executive Director:</td>
<td>Director of Information and Digital Technology</td>
</tr>
<tr>
<td>Endorsing Body:</td>
<td>Healthcare Quality Assurance and Improvement Committee</td>
</tr>
<tr>
<td>Governance or Assurance Committee</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Implementation Date:</td>
<td>September 2010</td>
</tr>
<tr>
<td>Version Number:</td>
<td>2.6.4</td>
</tr>
<tr>
<td>Review Date:</td>
<td>September 2020</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

2. AIM, PURPOSE AND OUTCOMES

3. SCOPE
   3.1 Who is the Policy Intended to Benefit or Affect
   3.2 Who are the Stakeholders

4. PRINCIPAL CONTENT

5. ROLES AND RESPONSIBILITIES

6. RESOURCE IMPLICATIONS

7. COMMUNICATION PLAN

8. QUALITY IMPROVEMENT – MONITORING AND REVIEW

9. EQUALITY AND DIVERSITY IMPACT ASSESSMENT

10. SUMMARY OF POLICY / FAQS

11. REFERENCES – APPENDIX 1
CONSULTATION AND DISTRIBUTION RECORD

Contributing Author / Authors:  
- Alan Ashforth, Information Security Manager, eHealth

Consultation Process / Stakeholders:  
- Donald Wilson, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)  
- Information Governance Committee members

Distribution:  
- All staff

CHANGE RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Change</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2006</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Mar 2007</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Sept 2010</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>2.0</td>
</tr>
<tr>
<td>May 2013</td>
<td>A Ashforth</td>
<td>Revised in view of comments</td>
<td>2.2</td>
</tr>
<tr>
<td>May 2014</td>
<td>A Ashforth &amp; C</td>
<td>Revised in view of comments</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>Tannahill</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Aug 2014   | A Ashforth & C  | Main change - Insertion of new sub-section 4.6.2.2 Protection of Media/Device and Transportation of Data  
|            | Tannahill       | Minor change - Reference appendix updated                              |             |
| Aug 2015   | A Ashforth      | Minor change - Reference appendix                                       | 2.5         |
| April 2017 | A Ashforth      | Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation. | 2.5.2       |
| April 2018 | A Ashforth      | Reviewed in line with General Data Protection Regulation (GDPR)        | 2.6         |
| June 2018  | A Ashforth      | Updated to show new director of information and digital technology     | 2.6.1       |
| Aug 2018   | A Ashforth      | Updated reference to Data Protection Act 2018                          | 2.6.2       |
| Sept 2018  | A Ashforth      | Data protection statement added into Section 3 - Stakeholders          | 2.6.3       |
| Oct 2018   | A Ashforth      | Adapt IS policy for use in General Practice                            | 2.6.4       |
| May 2020   | K. Torrance     | Extended until September 2021 (COVID-19)                               | 2.6.4       |
1. **Introduction**

This policy relates to secure use of removable storage devices and forms part of the overall Information Security policy for NHS Lanarkshire.

All removable media for use on information systems owned or operated by NHSL are covered by this policy.

This policy covers all types of NHSL owned portable IT equipment including laptops, removable storage media, PDA’s and smart phones.

2. **Aim, Purpose and Outcomes**

- Ensure that INFORMATION SECURITY is maintained
- Ensure that confidentiality and integrity of personal and sensitive information is maintained
- Ensure that information is available to **authorised** users
- Ensure that information is not disclosed to **unauthorised** people
- Ensure the safe **destruction** of information where appropriate
- Ensure the safe storage and transportation of removable media devices
- Ensure that information is safeguarded on the removable media devices
- To advise staff of their obligations to maintain information confidentiality, integrity, and availability

This policy forms part of eHealth Information Security Management System (ISMS) and should be read in conjunction with all the IS policies.

This policy has been written in line with the best practice for information security standards ISO 27001 and ISO 27002 and the policy will be reviewed to meet future changes to this standard.

This policy has been written to comply with current legislation and the policy will be updated appropriately to suit new and/or modified legislation. The references appendix will be updated to reflect this legislation.

3. **Scope**

3.1 **Who is the Policy intended to Affect?**

This policy is intended for all NHS Lanarkshire staff to maintain information security. In the interests of clarity all references to ‘staff’ includes all staff within NHS Lanarkshire and all staff who are employed, engaged or partners within each GP practice (contracted to NHS Lanarkshire).

3.2 **Who are the Stakeholders**
Information Security Policy – Secure Use of Removable Storage Devices

All staff.

NHS Lanarkshire take care to ensure your personal information is only accessible to authorised people. Our staff have a legal and contractual duty to keep personal health information secure, and confidential. In order to find out more about current data protection legislation and how we process your information, please visit the Data Protection Notice on our website at www.nhslanarkshire.scot.nhs.uk or ask a member of staff for a copy of our Data Protection Notice.

4. **Principal Content**

4.1 **Types of Portable Equipment:**

4.1.1 Portable Computers: Laptops and Notebook Computers

4.1.2 Removal Media Devices: A portable device that can be used to store or move data. This includes USB (Universal Serial Bus) memory sticks, USB external hard drives, digital cameras, floppy disks, magnetic tapes, cassettes and dictation machines. It covers any device that can be used to copy, save or write data and can be removed from its location and restored onto another computer or network.

4.1.3 PDAs: These are palmtops or handheld PCs.

4.1.4 Smart Phones/Tablets: These are mobile phones that can be used to send and receive email and also have the functionality to link to the Internet. Examples of these devices are the Blackberry, Apple iPhone, Apple iPad, Samsung Tab2, Toshiba AT300 tablet.

4.2 **Security of Removable Media Organisational Responsibility**

4.2.1 All NHS Lanarkshire issued equipment is encrypted using approved NHSL encryption software.

4.2.2 Only NHSL owned and approved media should be used with NHSL equipment and networks.

4.2.3 Equipment must be security marked to allow identification.

4.3 **Threats to Portable Equipment**

4.3.1 Theft and Loss: The risk here is not only about the loss of the equipment, but of the potential data loss to the organisation. This may include person identifiable information, commercially sensitive or research data.

4.4 **Secure and Acceptable Use**

4.4.1 Authorisations: Staff must apply for the use of removable media such as Encrypted USB memory stick, External Hard Drive, Digital Camera and (writing of) CDs/DVDs using the IT Service Desk. A completed application form with line
4.4.2 When purchasing any form of removable media for use within NHSL, that purchase must be processed through the NHSL eHealth Department.

4.5 Data Storage: Laptops

4.5.1 Within NHS Lanarkshire all laptops provided have encryption software installed, this enables the use of the equipment for the safe storage of person identifiable data.

4.5.2 Best practice is for the data to be stored on centrally held network drives. The storage of personal identifiable data to an encrypted laptop is acceptable but staff should ensure when no longer required this should be transferred to and stored on the network drives.

4.6 Protection of Media/Device and Transportation of Data

4.6.2 To protect against loss staff should take reasonable precautions to ensure the security of the equipment whilst in their care, this includes:

4.6.2.1 Equipment and data must not be taken offsite unless the device has been encrypted using NHSL approved software.

4.6.2.2 Care should be taken when transporting equipment. For smaller items such as CD/DVD or USB key, it would normally be safer to keep the media with you. For larger equipment such as a removable hard drive or laptop, it may be necessary to leave the equipment in a car, if doing so, it should be placed in the boot and the car locked. In the case of a car which has no cover over the boot such as an estate car, the equipment should not be visible to passers-by. The storing of equipment in a car should not be for extended periods of time such as overnight, it is much safer for the portable computer to be brought into your home.

4.6.2.3 It would be considered reasonable that general household security should ensure the safe storage of equipment. Where possible the equipment should be stored hidden from sight.

4.6.2.4 Staff should take care when carrying equipment in public places i.e. public transport, reception areas etc. this is to prevent accidental loss.

4.6.2.5 Portable computers, PDA’s and removable media are your responsibility at all times and you need to take all reasonable steps to keep the equipment secure.

4.6.2.6 DO NOT leave password details with any portable removable device.
4.6.2.7 Prevent unwanted access by locking your computer (CTRL, ALT, DELETE then select Lock).

4.6.2.8 Laptops and other removable media remaining in the workplace should be stored securely in the office drawer, filing cabinet or secured via cable lock system when not required.

4.7 Bulk transfer of data using removable encrypted storage devices or using NHSL approved electronic methods:

4.7.1 Data transfers using these secure methods are allowed provided there are additional security measures that have been considered. The transfer can be internally within NHS Lanarkshire or external to the organisation. The transfer must be done safely and securely. The factors to be considered are:

4.7.1.1 This is the only method and no alternative is available.

4.7.1.2 The only acceptable removable encrypted storage devices are those purchased and authorised for this purpose by NHSL.

4.7.1.3 The encrypted removable storage device drive should be transported securely by hand delivery or using an agreed and approved NHSL courier.

4.7.1.4 If data is transferred electronically an NHSL approved tool must be used to encrypt the data prior to any transmission.

4.7.1.5 For internal transfer the preference would be by hand delivery.

4.7.2 External transmission, additional security measures require to be considered.

4.7.2.1 Is there further approval required prior to sending?

4.7.2.2 What safety measures are in place to ensure the secure transmission of data – electronically or by removable encrypted storage device?

4.7.2.3 Are non-disclosure agreements in place with the external recipient of the data? This is to ensure that the company are also compliant with Information Governance and Information Commissioners Office Registration.

4.7.2.4 Authorisation for non routine removal of media or data from NHS Lanarkshire system must be obtained before removal and a record must be kept of all removals in order to maintain an audit trail.

4.7.2.5 Any bulk extracts of confidential or sensitive data must be authorised by the Information Governance Manager prior to any data of this type being removed from NHSL.
4.7.2.6 All media must be stored in a secure environment.

4.7.2.7 If further information is required the contacts are the Information Security Manager for the secure transfer of data and the Information Governance Manager for the compliance with Information Governance.

4.8 Responsibilities

4.8.1 Line managers are responsible for the day-to-day management and supervising the use of removable media within their work areas to ensure this policy is followed.

4.8.2 Staff who have been authorised to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as required by this policy.

4.9 Disposal

4.9.1 When the business purpose has been satisfied, the contents of removable media must be removed from that media through a destruction method that makes the recovery of the data impossible. Alternatively, the removable media and its data should be physically destroyed. In either case the removal media must be returned to eHealth so that appropriate action is taken. In all cases, a record of the action to remove data from or to destroy data should be recorded in an auditable log file.
5. **Roles and Responsibilities**

Authors/Contributors: Information Security Manager, eHealth
Executive Director: Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body: Information Governance Committee

6. **Resource Implications**

No resource implications

7. **Communication Plan**

This policy will be managed through the Corporate Policies intranet site and will be announced through the staff briefing.

8. **Quality Improvement – Monitoring and Review**

To be reviewed at regular intervals by Information Security Manager.

9. **Equality and Diversity Impact Assessment**

This policy meets NHS Lanarkshire’s EDIA

10. **Summary of Frequently Asked Questions (FAQs)**

N/A

11. **References Appendix 1**

The principal Acts of Parliament, Scottish Government circulars, and internal guidance documents relevant to this policy are:

- General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- NHSL Risk Management Strategy 2016
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012
Information Security Policy – Secure Use of Removable Storage Devices

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000