Information Security Policy  
Asset Management of Client 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>
Contents

i) Consultation and Distribution Record  
ii) Change Record

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
Information Security Policy – Asset Management of Client Devices

CONSULTATION AND DISTRIBUTION RECORD

<table>
<thead>
<tr>
<th>Contributing Author / Authors</th>
<th>Alan Ashforth, Information Security Manager, eHealth</th>
</tr>
</thead>
</table>
| 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 Tannahill</td>
<td>Revised in view of comments, Minor change - Reference appendix updated, Minor change - some rewording throughout</td>
<td>2.3</td>
</tr>
<tr>
<td>Aug 2014</td>
<td>A Ashforth &amp; C Tannahill</td>
<td>Minor change - Reference appendix updated, Minor change - some rewording throughout</td>
<td>2.4</td>
</tr>
<tr>
<td>Aug 2015</td>
<td>A Ashforth</td>
<td>Minor change - Reference appendix</td>
<td>2.5</td>
</tr>
<tr>
<td>Oct 2016</td>
<td>A Ashforth</td>
<td>Renamed policy from ‘Secure Use of Personal Computers to Secure Use of Client Devices’. References to personal computers changed to client devices to include desktop computers, laptops and tablets</td>
<td>2.5.2</td>
</tr>
<tr>
<td>April 2017</td>
<td>A Ashforth</td>
<td>Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.</td>
<td>2.5.3</td>
</tr>
<tr>
<td>April 2018</td>
<td>A Ashforth</td>
<td>Reviewed in line with General Data Protection Regulation (GDPR)</td>
<td>2.6</td>
</tr>
<tr>
<td>June 2018</td>
<td>A Ashforth</td>
<td>Updated to show new director of information and digital technology</td>
<td>2.6.1</td>
</tr>
<tr>
<td>Aug 2018</td>
<td>A Ashforth</td>
<td>Updated reference to Data Protection Act 2018</td>
<td>2.6.2</td>
</tr>
<tr>
<td>Sept 2018</td>
<td>A Ashforth</td>
<td>Data protection statement added into Section 3 - Stakeholders</td>
<td>2.6.3</td>
</tr>
<tr>
<td>Oct 2018</td>
<td>A Ashforth</td>
<td>Adapt IS policy for use in General Practice</td>
<td>2.6.4</td>
</tr>
<tr>
<td>March 2020</td>
<td>K. Torrance</td>
<td>Extended until September 2021 (COVID-19).</td>
<td>2.6.4</td>
</tr>
</tbody>
</table>
Information Security Policy – Asset Management of Client Devices

1. Introduction

This policy relates to asset management of client devices and forms part of the overall Information Security policy for NHS Lanarkshire.

Aim, Purpose and Outcomes

To ensure that all NHS Lanarkshire client devices are maintained in an asset register showing equipment location and authorised staff.

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

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.
Information Security Policy – Asset Management of Client Devices

4. Principal Content

Asset Marking
- All client devices such as desktop computers, laptops and tablets will be asset tagged by eHealth staff. NHS Lanarkshire (NHSL) staff deploying such equipment will use an asset label. The label will show an asset number of the format NHSL99999 e.g. NHSL01021, or D99999 (for desktop), or M99999 (mobile device – laptop/tablet). This will be used to identify all client devices in NHSL. Support calls to the IT Service Desk will require a note of the asset tag for the client device.
- The Asset Management Database will record the asset numbers of the client device, as well as details of the staff of the device. A scheduled and automated detailed hardware and software audit is performed to assist in software licence compliance and general user support.

Tracking
- To maintain an accurate audit of computer equipment and allocated staff. A request should be made on the IT Service Desk where:
  - a) A relocation of a client device such as desktop computer, laptop or tablet is required.
  - b) There is a return or transfer of a client device such as desktop computer, laptop or tablet staff or department.
- Where commercial companies wish to make donations of IT equipment to NHSL, those receiving such equipment must inform the eHealth Department. This is to allow such equipment to be managed as a NHSL asset.
- The purchase of all new IT equipment must be procured centrally through the eHealth Department.

Disposal of NHSL Client Devices
- All NHSL computer equipment deemed no longer suitable for use by the eHealth department is to be disposed of in a secure manner.
- NHSL eHealth Department will ensure that all hard drives in client devices and servers are disposed of permanently by physical shredding.
- Where NHSL uses the services of an external agency to perform this destruction the eHealth department will be responsible for receiving “Certificates of Destruction” from such an agency as proof of destruction.
- All certificates of destruction will list the asset tag of the destroyed equipment. This will subsequently be used to flag such equipment as destroyed on the asset management database.
- All back-up media deemed no longer fit for purpose will be physically destroyed on NHSL premises prior to final disposal.
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 – Asset Management of Client Devices

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