# Information Security Policy

**Secure Use of Client Devices**

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

12. CLIENT DEVICE SECURITY SUMMARY OF GOOD PRACTICE – APPENDIX 2
### 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>Aug 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</td>
<td>2.3</td>
</tr>
</tbody>
</table>
| Aug 2014   | A Ashforth & C Tannahill| Main change - rewording of sub-section 4.3.2  
Minor change - Reference appendix updated  
Minor change - some rewording throughout | 2.4         |
| Aug 2015   | A Ashforth              | Minor change - Reference appendix                                       | 2.5         |
| Oct 2016   | A Ashforth              | 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 | 2.5.2       |
| April 2017 | A Ashforth              | Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation | 2.5.3       |
| 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 Client Devices and forms part of the overall Information Security policy for NHS Lanarkshire.

2. **Aim, Purpose and Outcomes**

To 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
- To prevent **destruction** of information

Advising staff of their obligations to maintain information confidentiality, integrity, and availability.

This policy forms part of the 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](http://www.nhslanarkshire.scot.nhs.uk) or ask a member of staff for a copy of our Data Protection Notice.
4 Principle Content

This provides advice and guidance in respect of protecting the equipment and information stored on client devices. Appendix 2 of this document has good practice guides for client device security.

4.1 Acquisition of client devices including Desktop PCs, Laptops, PDAs, Smart Phones

4.1.1 The acquisition, maintenance, management and disposal of all computer assets (hardware, operating software and proprietary software) is performed centrally by the eHealth Department.

4.1.2 This aims to ensure that computer hardware and software is, as far as is possible, compliant with current NHS Lanarkshire (NHSL) eHealth strategy. Centralised purchasing and supply of systems by the eHealth department allows more cost effective purchasing of hardware, software and deployment of security controls.

4.1.3 NHSL will only support computer equipment procured by NHSL, or gifted to NHSL, and treated as NHSL assets.

4.2 Security

4.2.1 Each computer user must take personal responsibility for the security of the equipment and data in his/her care. Reasonable precautions must be taken to protect computer equipment from theft or inappropriate access.

4.2.2 A computer must only be opened (to expose its electronic components) and worked on by authorised staff and maintenance engineers. Opening a computer not only exposes the equipment to possible damage, but also opens the possibility that an unqualified member of staff may be harmed by, for example, an electric shock.

4.2.3 Only authorised software provided by NHSL may be installed onto a computer.

4.2.4 Software must not be removed or copied from a NHSL computer for loading onto another computer, without authorisation from the eHealth Department.

4.2.5 NHSL has centralised most data therefore staff should be using network drives for saving files. These network drives exist as a central resource available to NHSL staff for hosting data securely. This resource is highly available, backed up, and the data replicated to a secondary site, so there should be no need to keep a separate backup of this data.

4.2.6 When leaving a Windows based client device unattended it must be secured by locking the client device by pressing CTRL+ALT+DEL and selecting LOCK COMPUTER, or Windows+L.

4.2.7 Staff must not develop applications without the formal approval of eHealth.
4.3 Portable Client devices (Laptops, PDAs, Smart Phones etc)

4.3.1 All NHSL laptops utilise whole disk encryption to restrict access to data saved on the laptop to authorised staff only. NHSL utilises encryption to all portable storage devices such as PDA’s and Smart Phones where possible.

4.3.2 All reasonable precautions should be made to keep a portable client device secure. This is particularly important when in public areas such as public transport. If it is necessary to leave a portable client device in a car 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 portable client device should not be visible to passers-by. The storing of portable client device in a car should not be for extended periods of time such as overnight, it is much safer for the portable client device to be brought into your home.

4.3.3 The user is responsible for ensuring that no unauthorised person has access to the portable client device and this includes access by family members when the portable client device is used at home.
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
- NHS Lanarkshire’s 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 Client Devices

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

12. Client Device Security Summary of Good Practice - Appendix 2

The user of any computer must:

- be responsible for the security of the client device
- switch off client devices including desktops, laptops, tablets and peripheral equipment (printers, scanners etc.) when not in use
- ensure that no unauthorised persons use the client device
- not deliberately use any unofficial, unauthorised or unlicensed software
- if you have local data on your client device, back it up regularly to the R or T drive
- be aware of, and familiar with, the requirements of the current data protection legislation. For further information contact your Information Governance Manager
- secure portable client devices when unattended in an unlocked area within the workplace
- take all reasonable steps to minimise the visibility of client device equipment from outside the home, and to secure windows and doors when the home is unoccupied
- should not leave a portable client device in a car be for extended periods of time such as overnight, it is much safer for the portable client device to be brought into your home.