Information Security Policy
Asset Management of Client Devices

Author:	**Information Security Manager**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Quality Assurance and Improvement Committee**
Governance or Assurance Committee	**Information Governance and Cyber Assurance Committee**
Implementation Date:	**September 2010**
Version Number:	**2.6.6**
Last Review Date:	**Dec 2023**
Review Date:	**Dec 2026**

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

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Alan Ashforth, Information Security Manager
Consultation Process / Stakeholders:	• Donald Wilson, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance and Cyber Assurance Committee
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
Mar 2006	A Ashforth	Revised in view of new policy template	1.0
Mar 2007	A Ashforth	Revised in view of new policy template	1.0
Sept 2010	A Ashforth	Revised in view of new policy template	2.0
May 2013	A Ashforth	Revised in view of comments	2.2
May 2014	A Ashforth & C Tannahill	Revised in view of comments	2.3
Aug 2014	A Ashforth & C Tannahill	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	Reviewed in line with SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)	2.5.1
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

June 2021	A Ashforth	Scheduled review including updated UK GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section	2.6.5
Dec 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. References Appendix 1 – updated.	2.6.6

1. Introduction

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

2. 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 the 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.

4. Principal Content

Asset Marking

- All client devices such as desktop computers, laptops and tablets will be asset tagged by Digital 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 Digital. 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 Digital.

Disposal of NHSL Client Devices

- All NHSL computer equipment deemed no longer suitable for use by the Digital department is to be disposed of in a secure manner.

- Digital 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, Digital 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
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance and Cyber Assurance 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

X

(tick box)

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:

- UK General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- National Cyber Security Centre Cyber Assurance Framework
- Scottish Government Public Sector Cyber Resilience Framework
- CEL 25 (2012) NHS Scotland Mobile Data Protection Standard
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- MEL 2000 (17) Data Protection Act 1998
- NHSL Risk Management Framework
- 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
- SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000