Information Security Policy
Secure Use of Data Network

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 Committee**
Implementation Date:	**September 2010**
Version Number:	**2.6.5**
Last Review Date:	**Aug 2021**
Review Date:	**Aug 2024**

CONTENTS

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

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 2012	A Ashforth	Revised in view of comments	2.1
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	Main change - rewording of Network Security and Your Computer section 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	New paragraph – Network Segregation	2.5.1
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)	2.5.2
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

1. Introduction

This policy relates to Data Network and Internet Services 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

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

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

Access to the NHSL Data Network

When a new member of staff begins work in NHSL their manager must log a call with the IT Service Desk requesting an account for this individual providing the full name and job title in the call.

NHSL monitors network usage on an individual user basis. In the event that a member of staff is found to be in breach of the policy NHSL may take action in accordance with the appropriate HR policies.

The NHSL network is private and secure and all outgoing and incoming connections from/to NHSL are via the corporate firewalls managed by eHealth and their contractors, the connection of modems or routers is strictly prohibited unless authorised by the General Manager of eHealth.

Guidelines for using the NHSL Data Network

Acceptable use of the NHSL network includes:

- Purposes directly associated with the main Healthcare and linked support activities of NHSL.
- Communication and exchange for professional development, to maintain currency, or to debate issues in a field or sub field of knowledge.
- Recreational use of the Internet (excluding on-line gaming on the Internet) should take place during recognized break times and is at the discretion of your line manager.

Unacceptable use of the NHSL network connection includes, but is not limited to:

- Accessing, storing, sending, creating or displaying obscene or offensive data, even temporarily, unless for legitimate business purpose e.g. child protection.
- Deliberate transmission of any material in violation of any United Kingdom law is prohibited. This includes, but is not limited to copyrighted material (unless authorised by the copyright holder), threatening or obscene material, or material protected by trade secret, unless for legitimate business purpose e.g. child protection.
  - Any activities that benefit any political or commercial organisation that is not approved by the NHSL Partnership Forum.
  - Any activities that are for personal profit unless in connection with NHSL business purpose.

- Staff must not **deliberately** endanger the proper working of computer equipment and software, it is accepted that mistakes can happen! 'Hacking' and other unauthorised use of computing equipment, whether situated on NHSL premises or elsewhere, is explicitly forbidden. These points are in keeping with the Computer Misuse Act 1990. A NHSL member of staff should not attempt to access any computer or computer system using the NHSL network, either within NHSL, other NHS Scotland or non NHS Scotland organisations, without the prior knowledge of and approval from properly authorised persons responsible for the computer or computer systems to be accessed.

- Deliberate activities with any of the following characteristics:

  - Corrupting or destroying other staff data;

  - Using network facilities to **deliberately** disrupt the work of other staff;

  - Continuing to use an item of networking software or hardware after the NHSL has requested that use cease because it is causing disruption to the correct functioning of the network;

  - Endangering network services through the **deliberate** introduction of "computer viruses".

- The NHSL network should not be used for the development of computer applications, including web-based systems that are not for the explicit Healthcare and associated purposes of the NHSL.

NHSL Staff and Network Security

The Internet or World Wide Web is outside the NHSL network. In contrast to the Internet, the NHSL network can be thought of as a secure area. Any information sent or received via the Internet has to be viewed as being in the public domain and hence outside this secure area. Information sent and received in this way can potentially be read by anyone else connected to the Internet. Thus, the sending of PID (Person Identifiable Data) or other sensitive information from the NHSL network onto recipients outside NHSL is strictly prohibited unless this has been authorised by your line manager and meets the requirements of the NHSL Information Security Policies. Refer to E-Mail and Internet usage policies for more information.

Network Segregation

It may be necessary to use physical and logical segmentation to protect the organisations information and assets (e.g. patient identifiable information). Traffic between segments including allowed external parties, should be controlled in accordance with the need to transmit/receive information. Gateways, firewalls, and routers should be configured based on information classification.

Network Security and Your Computer

Only authorised staff have access to the network, you must safeguard access by electronically locking or logging out of Microsoft Windows. The Secure Use of Personal Computers policy includes an appendix that provides a good practice guide for protecting the information on your computer.

You should take appropriate sensible measures to protect your computer from viruses. The eHealth Department is responsible for centrally managing anti-virus software on behalf of all NHSL staff. Nevertheless staff should take care when they receive computer media as it could contain a virus, and should contact the IT Service Desk for advice.

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 ☒ (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)
- Scottish Health Competent Authority - NCSC Cyber Assurance Framework
- Scottish Health Competent Authority - Information Security Policy Framework (ISPF) 2018
- Scottish Government Public Sector Cyber Resilience Framework
- Scottish Government Public Sector Action Plan 2017-18
- 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 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
- 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