Information Security Policy
Secure Wireless Connectivity

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	1.2
May 2011	A Ashforth	Rewritten in view of new wireless infrastructure	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	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	New paragraph – Network Segregation	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 Wireless Connectivity 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

The purpose of this policy is to define the standards, procedures and restrictions that staff must adhere to in order to connect and use the NHS Lanarkshire (NHSL) IT wireless service appropriately.

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).

This policy applies to all staff, external IT contractors, suppliers and agencies who are provided by the NHSL eHealth Department with access to the NHSL wireless service and the IT services made available via connection to the NHSL network.

All transactions using this service are covered by this policy.

This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the NHSL network.

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

Supported Technology

Access to the NHSL wireless service can be provided to staff using a wireless enabled NHS Lanarkshire (NHSL) provided portable computer.

This policy refers to the wireless network installed and managed by the eHealth department in NHSL locations. This is the only authorised wireless infrastructure within NHSL.

Not all NHS Lanarkshire locations have wireless infrastructure, presently access points are mainly confined to the acute hospitals and headquarters offices in NHSL.

Wireless networks within NHSL locations should not be considered a replacement for a wired network. They should be utilised where a requirement exists for flexibility and mobility, such as in clinical areas, or in an office environment such as a meeting room.

Eligible Staff

All staff requesting access to the wireless service for business use only purposes must request this via the IT Service Desk on https://nhslanarkshireprod.service-now.com/sp or by contacting the IT Service Desk by telephone. The IT Service Desk must receive approval from the Line Manager of the requesting employee (an email approval is acceptable) before the request can be assigned to arrange installation setup for the user.

Policy and Appropriate Use

It is imperative that the wireless service is used by staff appropriately, responsibly and ethically at all times. The following rules of use must be adhered to by staff at all times:

1. Staff must take physical security precautions both to keep the computer equipment safe but also to keep sensitive content such as person identifiable data (PID) secure and not to allow unauthorized persons access to such data. This is particularly relevant in more public areas such as meeting rooms or a canteen/bistro for example.

2. Staff agree to and accept that their wireless connection to the NHSL network will be monitored to record dates, times, duration of access, etc., in order to identify any unusual usage patterns or other suspicious activity. This will be undertaken in order to identify accounts/computers that may have been compromised and represent a security risk to NHSL.

3. The installation and configuration any other wireless networks within NHSL are strictly forbidden.

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.

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 [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)
- 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