Information Security Policy
Intranet Acceptable Use

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 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
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.2
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	2.6.5

		GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section	

1. Introduction

This policy relates to Intranet Usage and forms part of the overall Information Security policy for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

2.1 The purpose of this policy is to ensure the responsible use of the NHS Lanarkshire's (NHSL's) Intranet access service. Whilst NHSL recognises the human rights of all staff its policy is to treat all electronic data that is stored on its computer network including all files relating to Intranet access as the property of NHSL and it reserves the right to inspect any and all files stored in our network in order to assure compliance with this policy. An **intranet** is a private computer network to share information, operational systems, or computing services within an organization

2.2 This is to:

2.2.1 Ensure that INFORMATION SECURITY is maintained

2.2.2 Ensure that confidentiality and integrity of personal and sensitive information is maintained

2.2.3 Ensure that information is available to *authorised* users

2.2.4 Ensure that information is not disclosed to *unauthorised* people

2.2.5 Ensure safe *destruction* of information where appropriate

2.2.6 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

4.1 The use of any NHSL resource for illegal activity is grounds for disciplinary action according to local disciplinary procedures and NHSL will co-operate with any legitimate law enforcement activity and NHSL will co-operate with any legitimate law enforcement activity.

4.2 NHSL retains the copyright to any material posted by any employee in the course of his or her duties. This is inclusive of the Intranet.

4.3 Sensitive Intranet content should never be openly displayed to those not authorised or required to see it.

4.4 Use of NHSL Intranet access facilities to commit any breach such as misuse of NHSL's assets or resources, sexual harassment and misappropriation or theft of intellectual property are also prohibited.

4.5 Audits to ensure compliance with this policy may be undertaken at any time by suitable authorised personnel with or without prior notice. If there is evidence that an individual is not adhering to the guidelines set out in this policy, NHSL reserves the right to remove Intranet access and to advise the respective Line Manager of this evidence. The Line Manager will undertake the appropriate disciplinary action consistent with their local disciplinary procedures.If the person identified has unreasonable or offensive intranet access, and they are a member of a GP Practice, the practice manager will be made aware that the individual has breached this policy. Should a GP be identified regarding a severe finding and/or illegal activity, then this will be reported to the appropriate Medical Director for Health and Social Care Partnership.

4.6 If you have good reason to suspect anyone is deliberately disregarding this policy then you should report your suspicions to your supervisor, the IT Service Desk or any other member of the eHealth department. All such reports will be treated in strict confidence.

4.7 Surveys & Discussion Forums:

4.7.1 These features may be created and published by nominated department personnel who have been assigned the proper administrative, access permissions. Use of these features is at the discretion of department managers for the legitimate, business use of the department and must be vetted and authorised electronically within the intranet application by the head of department before being published.

4.7.2 Creating surveys and discussion forums for inappropriate purposes or responding to them in an inappropriate manor will contravene this policy

4.8 Social Issues and Events Section:

4.8.1 The Social Issues and Events section of the intranet is intended to encourage use of the intranet by informing staff of useful information and to promote participation and membership of various social staff events and clubs which may be of interest to staff.

4.8.2 This section may be used to advertise and promote social events including sports or hobby clubs set up by and for staff participation. Although this information may not be directly related to their jobs, action may be taken if any misuse of this section for inappropriate content.

4.9 External Contractors, and third parties including GP's and practice staff

4.9.1 The above parties are expected to fully comply with the terms and conditions of this document whilst connecting to NHSL's networking infrastructure. Failure to comply or a show of disregard for the terms and conditions of this document may be interpreted as a threat to compromise the security of NHSL's computer network.

4.9.2 In such an event it would be expected that an eHealth representative would apprise the respective Line Manager (Practice Manager / Responsible Partner) of the situation. If the matter is not satisfactorily resolved then NHSL would reserve the right to terminate the individuals' access to NHSL's computer network with immediate effect.

4.9.3 If you have any questions or comments about this Intranet Access Policy, please contact your supervisor or IT Service Desk.

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

To be deployed by Policy Management System.

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