# Information Security Policy
## Internet Acceptable Use

**Information Security Policy – Internet Acceptable Usage**

<table>
<thead>
<tr>
<th>Author:</th>
<th>Information Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Lead Executive Director:</td>
<td>Director of Information and Digital Technology</td>
</tr>
<tr>
<td>Endorsing Body:</td>
<td>Healthcare Quality Assurance and Improvement Committee</td>
</tr>
<tr>
<td>Governance or Assurance Committee</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Implementation Date:</td>
<td>September 2010</td>
</tr>
<tr>
<td>Version Number:</td>
<td>2.6.4</td>
</tr>
<tr>
<td>Review Date:</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
## 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>May 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 section 4.2  
Minor change - Reference appendix updated  
Minor change - some rewording throughout                             | 2.4         |
| Feb 2015 | A Ashforth              | Removed repeated point 4.11 authorisation to speak with the Media     | 2.5         |
| Mar 2015 | A Ashforth              | Minor change to provide wording point 4.21.3 ‘NHSL does not take responsibility for any personal financial loss if individuals use electronic banking, or debit card/credit card based transactions, and as such individuals do this at their own risk’. | 2.5.1       |
| Aug 2015 | A Ashforth              | Minor change - Reference appendix                                     | 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. | 2.5.4       |
| 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       |
Information Security Policy – Internet Acceptable Usage

1. Introduction

This policy relates to Internet Acceptable 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) Internet 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 Internet 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.

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](http://www.nhslanarkshire.scot.nhs.uk) or ask a member of staff for a copy of our Data Protection Notice.

4. **Principal Content**

4.1 NHSL has software and systems in place that are capable of monitoring and recording all Internet usage.

4.2 The display of any kind of sexually explicit image or document on NHSLs systems is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources. The only exception to this is for legitimate business activity.

4.3 NHSL uses independently-supplied software and data to identify inappropriate Internet sites. We may block access from within our network infrastructure to all such sites these include gambling, gaming or sexually explicit websites.

4.4 If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately.

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

4.6 Any software or files downloaded via the Internet into NHSL’s network may be used only in ways that are consistent with their licenses or copyrights. Illegal use of software on any of NHSL’s systems is strictly prohibited.

4.7 No employee may use NHSL computer facilities knowingly to download or distribute illegally acquired software or data of any nature including audio and visual files.

4.8 Internet sites can be infected with computer viruses. If you use the Internet and subsequently your PC/laptop exhibits consistent strange behaviour contact the IT Service Desk immediately. The strange behaviour could indicate the presence of a computer virus on your PC/laptop.
4.9 No employee may use NHSL’s Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

4.10 No employee may use NHSL’s Internet facilities knowingly to disable or overload any computer system or network, or to bypass any system intended to protect the privacy or security of another user.

4.11 Staff may participate in newsgroups or chat rooms in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves.

4.12 Each employee using the Internet facilities of NHSL shall identify himself or herself honestly, accurately and completely (including one’s organisation affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on external systems.

4.13 Staff are reminded to be careful when using chat rooms and newsgroups as public forums as not to reveal confidential or sensitive NHSL information, patient data, and any other material covered by existing NHSL and NHS confidentiality policies and procedures. Staff releasing protected information in this way will be subject to local disciplinary procedures.

4.14 Where an individual participant is identified as an employee or agent of NHSL, the employee must refrain from any unauthorised political advocacy and must refrain from the unauthorised endorsement or appearance of endorsement by NHSL of any commercial product or service not sold or serviced by NHSL, the NHS, its subsidiaries or its affiliates.

4.15 Only those managers and NHSL officials who are authorised to speak to the media, to analysts or in public gatherings on behalf of NHSL may grant such authority to newsgroup or chat room participants.

4.16 NHSL retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.

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

4.18 Use of NHSL Internet access facilities to commit breaches such as misuse of NHSL assets or resources, sexual harassment, unauthorised public speaking and misappropriation or theft of intellectual property are also prohibited.

4.19 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 Internet 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 internet 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.

4.20 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.

4.21 Personal usage

4.21.1 Although NHSL’s Internet access capabilities are intended for business use, NHSL allows personal usage if it is reasonable and does not interfere with work e.g. lunch or other suitable work breaks.

4.21.2 However for the reasons given previously NHSL cannot guarantee personal privacy and reserves the right to halt such usage to any individuals found abusing the trust of NHSL.

4.21.3 The individual is solely responsible for the security of their personal use of the Internet such as Internet based banking passwords and displaying personal confidential information on screen. NHSL does not take responsibility for any personal financial loss if individuals use electronic banking, or debit card/credit card based transactions, and as such individuals do this at their own risk.

4.22 External Contractors, and third parties including GP’s and practice staff

4.22.1 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.

4.22.2 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 networking infrastructure and computer network with immediate effect.

4.22.3 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 Strategic Planning & Performance & Executive Lead for eHealth
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
- 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

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