Information Security Policy
Digital Visiting

<table>
<thead>
<tr>
<th>Authors:</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>May 2020</td>
</tr>
<tr>
<td>Version Number:</td>
<td>1.0</td>
</tr>
<tr>
<td>Review Date:</td>
<td>September 2022</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:          | Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) |
| 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>April 2020</td>
<td>A Ashforth</td>
<td>First Draft: New policy for staff and patients on the safe use of digital technology for patient visiting</td>
<td>0.1</td>
</tr>
<tr>
<td>April 2020</td>
<td>A Ashforth</td>
<td>Second Draft</td>
<td>0.2</td>
</tr>
<tr>
<td>May 2020</td>
<td>A Ashforth</td>
<td>Third Draft – modified focus and scope</td>
<td>0.3</td>
</tr>
<tr>
<td>May 2020</td>
<td>A Ashforth</td>
<td>Forth Draft – removed reference to NHS App as not relevant to NHS Scotland patients</td>
<td>0.4</td>
</tr>
<tr>
<td>May 2020</td>
<td>A Ashforth</td>
<td>Fifth Draft – created a new paragraph for safety – moved mobile device interference bullet into this section</td>
<td>0.5</td>
</tr>
<tr>
<td>June 2020</td>
<td>A Ashforth</td>
<td>Final version</td>
<td>1.0</td>
</tr>
</tbody>
</table>
1. **Introduction**

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

2. **Aim, Purpose and Outcomes**

The aim of this policy is to provide a consistent and robust advice to staff and patients on how to use digital technology for relatives to keep contact with loved ones.

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, and procedures to ensure the legal use of digital technology used by staff and patients.

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 for staff responsible for the care of patients and for patients in the use of mobile devices supplied by NHS Lanarkshire for digital visiting.

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.
Information Security Guidance – Digital Visiting

4. **Principal Content**

4.1 Background
This policy provides advice for patients using mobile devices supplied by NHS Lanarkshire.

This is particularly important during periods when the risk of infection between patients is higher and patients may be isolated from loved ones.

During this time patients should follow the advice of the Government and the NHS on washing your hands more regularly than usual and take appropriate precautions to ensure any mobile device you use is regularly cleaned.

It is recommended that patients do not share mobile devices with other patients within the ward to ensure control of infection.

4.2 Privacy and consideration of other patients and staff
NHS Lanarkshire want patients to use a mobile device in hospital, it’s an important way of keeping in touch.

It’s important that when patients use a mobile device in hospital they’re careful not to:

- Take anyone’s photo without permission, including staff or people in the background of your photos e.g. in busy waiting areas. It is important to remember that taking a photo or video could breach another patient’s privacy and cause them distress.

- Make video calls in a way that means the other person can see any other patients, visitors or staff members.

- Make calls or use your phone in a way that disturbs other patients.

4.3 Safety
It’s important that when patients use a mobile device in hospital they’re careful not to:

- Use your mobile device around sensitive equipment where there is a particularly high risk of interference. Signs will make it clear that you shouldn’t use your phone in that area. Switch it off or enable ‘airplane mode’. Do not just leave the device on the silent or vibrate setting as it could still affect medical equipment.

4.4 Managed device supplied by NHS Lanarkshire
eHealth have deployed iPads to a number of wards, and these are restricted to the apps called Zoom and Facetime. No other applications can be installed on these devices.

In order to protect patient data privacy, the device applications do not come with pre-defined accounts. Each patient will have the ability to log in and out with their own accounts and ensure that data is then not accessible to any other patient.
Information Security Guidance – Digital Visiting

**Zoom**
The policy provided with the device requires the relative creates an account and a meeting then provides the patient with the code to join. No accounts are saved on the device regarding zoom as it is effectively a single use meeting.

**Facetime**
The policy provided with the device requires the patient to have an Apple ID and password, this is entered into the Facetime app and once verified, the patient is able to make and receive Facetime calls.

A user guide will be provided with this device providing details on the full process for setting up Zoom or Facetime.

Devices will be provided to patients from NHS Lanarkshire as required during their stay within hospital.

Each device remains the property of NHS Lanarkshire and should be returned to ward staff on leaving the hospital.

Should support be required for the device, either software issues/configuration or hardware issues, staff should contact the eHealth service desk.

**4.5 Donations of portable tablet devices**
Donations of portable devices from charities, staff and relatives must **not** be accepted by staff. Similarly, staff should not purchase portable devices on behalf of the ward as these need to be purchased via eHealth, e.g. ward funds should not be used to directly purchase IT equipment.

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 Firstport 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 policy 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