Information Security Policy
Secure Use of Smartphone and Tablet Devices

Author:	**Information Security Manager**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Governance Committee**
Governance or Assurance Committee	**Information Governance and Cyber Assurance Committee**
Implementation Date:	**January 2025**
Version Number:	**2.7.4**
Review Date:	**Nov 2026**

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Information Security Manager
Consultation Process / Stakeholders:	• Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance and Cyber Assurance Committee
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
Jan 2014	A Ashforth	First draft	2.5
May 2014	A Ashforth	Updated draft	2.5.1
June 2014	A Ashforth	Draft modified reference to BYOD	2.5.2
Nov 2014	A Ashforth	Draft updated draft	2.5.3
Dec 2014	A Ashforth	Draft missing word “data” added to end of sentence at 4.3.2	2.5.4
Aug 2015	A Ashforth	Draft minor change – Reference appendix	2.5.5
Nov 2016	A Ashforth	Reviewed in line with SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)	2.5.6
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.7
July 2017	A Ashforth & J Duncan	Minor change – New bullet point 4.8 secure SMS (texting).	2.5.8
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

May 2022	A Ashforth	Remove reference to Airwatch. Added guidance on use of apps 4.9.	2.7
Sept 2022	A Ashforth	Updated 4.7.1 and 4.9.4 in view of comments from IG Committee members	2.7.1
Feb 2023	A Ashforth	Added new bullet point in 4.3 - Update for BYOD controls when accessing M365 Teams and/or M365 Email from personally owned devices	2.7.2
May 2023	A Ashforth	Added new bullet point in 4.10.4 - 'New apps will be reviewed by the Apps Governance Group.'	2.7.2
Nov 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. References Appendix 1 – updated.	2.7.3
Jan 2025	A Ashforth	Updated references appendix for broken link (from 'NHSL Risk Management Framework' with 'NHSL Risk Management Policy') and provided the updated link for the Scottish Government's Records Management Code of Practice. Change all references of 'IG Committee' to 'Information Governance & Cyber Assurance Committee (IG & CAC)' Change all references of 'Healthcare Quality Assurance and Improvement Committee' with 'Healthcare Governance Committee'	2.7.4

1. Introduction

This policy relates to Mobile Device Management and forms part of the overall Information Security policy for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

To ensure that all mobile devices used in NHS Lanarkshire for work purposes are managed effectively.

The purpose of this policy is to define standards, procedures, and restrictions for staff who have legitimate business uses for connecting mobile devices to NHSL's corporate network and data. This mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- Tablets (non-Windows)
- E-readers

Windows based tablets are managed in the same fashion as Windows based workstations and laptops refer to client device IS policies.

In order to maintain security and manageability, only devices using supported operating system versions are allowed to access corporate resources:

The purpose of this policy is to protect the integrity of data that resides within NHSL's IT Infrastructure. This policy intends to prevent data from being deliberately or inadvertently stored insecurely on a mobile device or sent over an insecure network where it could potentially be accessed by unauthorised parties.

A breach of this type could result in a direct impact on patient care through loss of data or unauthorised disclosure of data, and damage to NHSL's public image and reputation.

Therefore, all staff using a mobile device connected to NHSL's corporate network, and/or backing up, storing, or otherwise accessing corporate data of any type, must adhere to all of the NHSL defined policies and processes for doing so.

The policy addresses a range of threats to the organisations data, equipment or related to its use such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by a member of staff or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced to or via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the NHS Lanarkshire to the risk of non-compliance with various identity theft and privacy laws.

This policy forms part of the 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

It is the responsibility of each member of staff in NHSL who uses a mobile device to access corporate resources to ensure that they adhere to NHSL's Information Security Policies. Any mobile device that is used to conduct NHSL business is used appropriately, responsibly, and ethically. Failure to comply will result in the immediate suspension of that user's account and the device will be denied network access to these corporate resources.

Based on this requirement, the following rules must be observed:

4.1 Access Control

4.1.1 Digital reserves the right to refuse the ability to connect mobile devices to corporate infrastructure. Digital will engage in such action if such equipment is being used in a way that puts NHSL's IT systems, data and/or staff at risk.

4.2 Mobile Device Management (MDM)

4.2.1 NHSL's Digital Department uses a MDM, to secure and maintain control of mobile devices such as smartphones and tablets and enforce security policies on these devices remotely.

4.2.2 All corporate mobile devices are automatically enrolled in the MDM when the device is purchased, and this is applied at service provider level for secure access to corporate resources.

4.2.3 MDM enables Digital to take the following actions on mobile devices: remote data wipe, location tracking, application visibility and hardware management. The location tracking capability can be used if a device is lost or stolen.

4.2.4 MDM will install the following settings as part of the device enrolment on all Apple and Android devices:

- 6 digit pin.
  - Applied as soon as devices is enrolled
  - Does not allow simple PIN
  - Allow Touch ID or Face ID instead of PIN
  - Password history is set to 4
  - Auto lock 1 minute
  - Failed attempts = 8, then device wipe
- NHSS email settings.
- NHSL corporate wireless connection settings.

4.3 Personally Owned Device - BYOD (Bring Your Own Device)

4.3.1 NHSL now permit the use of personally owned smart phones & tablets for access to NHS Scotland MS 365 Teams and/or email using Microsoft apps. **This is the only approved use of BYOD within NHS Lanarkshire.** Staff wishing to use this service must download the following apps from their respective device manufacturers app store:

- Microsoft Teams
- Microsoft Outlook
- Microsoft Edge

This list is not exhaustive but includes the key corporate apps for mobile devices.

Staff should be aware of the following Mobile Application Management restrictions will be in place when using NHS Scotland MS Teams and Email using a personally owned device (BYOD):

- 6-character PIN or fingerprint enforced access to corporate apps such as MS Teams and Email – staff must NOT share this PIN with family members, and the corporate apps must NOT be accessed by family members and all other unauthorised people
- File share / export of documents to non-NHSS approved apps is blocked
- Embedded URLs are safe checked
- Embedded URLs will only open in Microsoft Edge
- Teams and Email notifications will not show details of the Teams postings or email e.g. Teams will provide a generic notification stating 'There is new activity', and the user will need to unlock the device to access the application to read the content

Staff using BYOD must be aware that they:

- Must NOT take screen shots as these will be saved locally on the device
- Must NOT take recordings of any personally identifiable patient or staff data (including photos, videos and audio) using the device
- May receive limited support from Digital. Any use of your own device is done so at your own risk and no replacements, repairs, updates and phone changes will be reimbursed by NHS Lanarkshire.

Staff participating in BYOD must be aware that in the course of an investigation into inappropriate conduct/use/management of NHS Lanarkshire data/systems, staff may be requested to temporarily surrender their personally owned device to the investigating manager. This is so that physical evidence is secured in the same way as an investigation process involving NHS Lanarkshire supplied devices. Staff who don't agree to this requirement must not utilise BYOD.

4.4 Security

4.4.1 Staff using mobile devices must adhere to the IS policies and this mobile device policy. Staff must ensure reasonable physical security measures are taken to prevent loss or inappropriate access.

4.4.2 In the event of a lost or stolen mobile device, it is a requirement for the user to report the incident to the Service Desk immediately and report the incident on Datix. The device will then be remotely wiped of all corporate data.

4.5 Hardware & Support

4.5.1 Staff will make no modifications to the hardware or software that change the functioning of the device in any significant way (e.g. replacing or overriding the operating system, jailbreaking/rooting[1]).

4.6 Organisational Protocol

4.6.1 Digital will establish audit trails which will be accessed, audited, and used without notice. These audit logs will be able to track the location of the mobile device. The resulting reports may be used for investigation of possible breaches and/or misuse. The staff member agrees to and accepts that his or her access and/or connection to NHSL's Digital Infrastructure may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The monitoring of the device, including additional capabilities; e.g. tracking application presence or usage, jailbreak detection, data usage, operating system version may also be monitored. This monitoring is required in order to identify compromised devices to reduce the risk of unauthorised access to NHSL systems and data.

4.6.2 The staff member must report immediately to their Line Manager and the Service Desk any incident, actual or suspected, relating to unauthorised data access, data loss, and/or disclosure of NHSL data assets.

4.6.3 Digital may supply a smartphone or tablet to a member of staff but only when the device is fully funded by the user department and line manager approval. Staff issued with a mobile device which has a SIM for use with both voice and data services will be fully responsible for the cost of all personal calls, as well as all data usage which exceeds the monthly data allowance.

4.6.4 The staff member's line manager must submit a Service Desk request to disable service as part of normal staff leaving and/or transferring processes.

4.7 Privacy

4.7.1 The nature of mobile devices and mobile device management installations is that a significant amount of user/device information is recorded. This includes location and usage data.

4.7.2 NHSL will not make routine use of this data. Access to this data is restricted to a very limited number of personnel and will only be used when the security of

1 # To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

the device has been compromised or when disclosures are required legally or as part of an investigation.

4.8 Cameras

4.8.1 Cameras in mobile devices are not to be used for recording of any personally identifiable patient or staff data (including photos, videos and audio) unless an Standard Operating Procedure (SOP) has been developed and this process risk assessed and discussed with the Information Governance Team, who may request a DPIA be completed before approval can be granted. Staff wishing to take images/recordings of patients and staff, should be aware of the Recordings (Photography and Video) for Clinical and Service Use Policy.

4.9 Secure SMS (Texting)

4.9.1 Information that has been classified as RED following the Records and Information Classification Scheme (RICS) protocol must not be text. If operational managers wish to implement SMS text as a means of communication for Amber and Green classified information, then they must risk assess their operational processes and discuss this with the Information Governance Team a with a view to develop an SOP and you may be asked to complete a DPIA for approval. SMS texting from Digital approved systems are exempt from this process. The Head of Information and Records Management should be contacted for advice on the application of the RICS protocol.

4.10 Apps

4.10.1 The MDM removes the app store functionality on all corporate mobile devices, so only approved applications can be installed from the Company Portal known as 'Comp Portal'.

4.10.2 An approved app could be a news app like BBC News or an alternative browser such as Google Chrome, or messaging or social media apps for example.

4.10.3 You are responsible for how you use an app for work the purposes. There are for example a number of caveats on the use of Microsoft 365 Teams and Email/Outlook and this guidance should be followed.

Social networking/ messaging apps are NOT approved for the recording of any personally identifiable patient or staff data, and that includes text, photos, videos and audio.

4.10.4 Staff can request Apps by raising an IT service request along with a business case on why the application is required. The Telecomms team will then review

the request and see if the application has already been requested or if it's a new request for an app.

- New apps will be reviewed by the Apps Governance Group.
- Existing approved applications can be pushed out or downloaded from the Comp Portal provided that the use of the app is compatible with the original approval. Apps previously approved but requested by another dept./team for a different use, may have to complete governance process again. By default, an SOP should also be in place by the service describing how they intend to use the app.
- Existing declined applications – users will be advised that the application has been declined in the past.

5. Roles and Responsibilities

Authors/Contributors:	Information Security Manager
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance and Cyber Assurance 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 EQIA [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)
- National Cyber Security Centre Cyber Assurance Framework
- Scottish Government Public Sector Cyber Resilience Framework
- 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 Policy
- Public Records (Scotland) Act 2011

- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management Code of Practice for Health and Social Care
- 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