NHS Shetland

Meeting:	**Shetland NHS Board**
Meeting date:	**15th February 2022**
Agenda reference:	**Board Paper 21/22/63**
Title:	**Digital Security Framework**
Responsible Executive/Non-Executive:	**Lorraine Hall**
Report Author:	**Craig Chapman**

1 Purpose

This is presented to the Board for:

- Awareness

This report relates to:

- Local policy

This aligns to the following NHSScotland quality ambition(s):

- Effective

2 Report summary

2.1 Situation

Cybersecurity is becoming an ever-increasing issue for public sector organisations. At the same time the use of digital technology to deliver services continues to increase.

The development and implementation of a Digital Security Framework is part of a wide-reaching set of strategies, policies, procedures and controls in place to protect the information held by NHS Shetland and sure appropriate access to it.

2.2 Background

NHS Shetland has information governance and security policies in place currently. However these require modernising to reflect both the increase risk to information assets and new legislation that places strict responsibilities on organisations for the secure storage and handling of this information. This legislation includes the **Data Protection Act (2018)** and the **Network and Information Systems Regulations (2018).**

NHS Shetland holds large quantities of highly sensitive data that it makes use of on a 24/7 basis to deliver healthcare.

2.3 Assessment

In order to ensure all digital security policy is clear and concise, it was decided to split each area into a separate, short, policy. By doing so staff can quickly find the information that pertains to their query, and any required changes to policy can be quickly implemented.

The organogram at the beginning of this framework shows all the relevant documents and how they are structured. **For clarity, this suite of documents is the Digital Security Strategy and associate polices (10 policies in total)**.

The overarching Information Governance Framework, The Information Governance Strategy and associated policies are under development.

2.3.1 Quality/ Patient Care

By ensuring staff have clear access to policy on all aspects of the use of digital technology, it follows that the quality of information recorded, how it is stored, and how it is managed will continue to improve. This has a direct impact on the quality of patient care and patient confidence in how we look after their data.

2.3.2 Workforce

If staff have clear guidance on the secure use of digital technology, and adhere to policy, they can be assured that they are handling information securely and are clear where to report concerns and issues, and where to seek guidance when required.

2.3.3 Financial

There is no direct financial implication of this framework, however there is potential for information security breach incidents to be reduced, therefore reducing costs associated with managing incidents.

2.3.4 Risk Assessment/Management

This framework is part of how NHS Shetland manages risk associate with digital security. By ensuring a robust approach to use of technology securely the organisation reduces it's risk exposure.

2.3.5 Equality and Diversity, including health inequalities

An impact assessment has not been completed.

2.3.6 Other impacts

The Digital Security Framework seeks to reduce risk and gives the organisation a clear mandate to address areas where non-compliant activity is identified. This may result in some group of staff or individuals having to change work practices that have historically been accepted. Both the Digital and Information Governance Departments will support staff with any changes to minimise impact on service delivery.

2.3.7 Communication, involvement, engagement and consultation

Staff have been consulted to provide professional input.

Communication to the wider organisation will be arranged following final completion of the Information Governance and Digital Security Framework i.e. when the framework is live.

The Digital Security Framework is relevant to the organisation and staff. Therefore no external engagement has been undertaken.

2.3.8 Route to the Meeting

This has been previously considered by the following groups as part of its development. The groups have either supported the content, or their feedback has informed the development of the content presented in this report.

- Information Governance Subgroup, October 2021
- Digital Informatics Support Group, 2nd November 2021

2.4 Recommendation

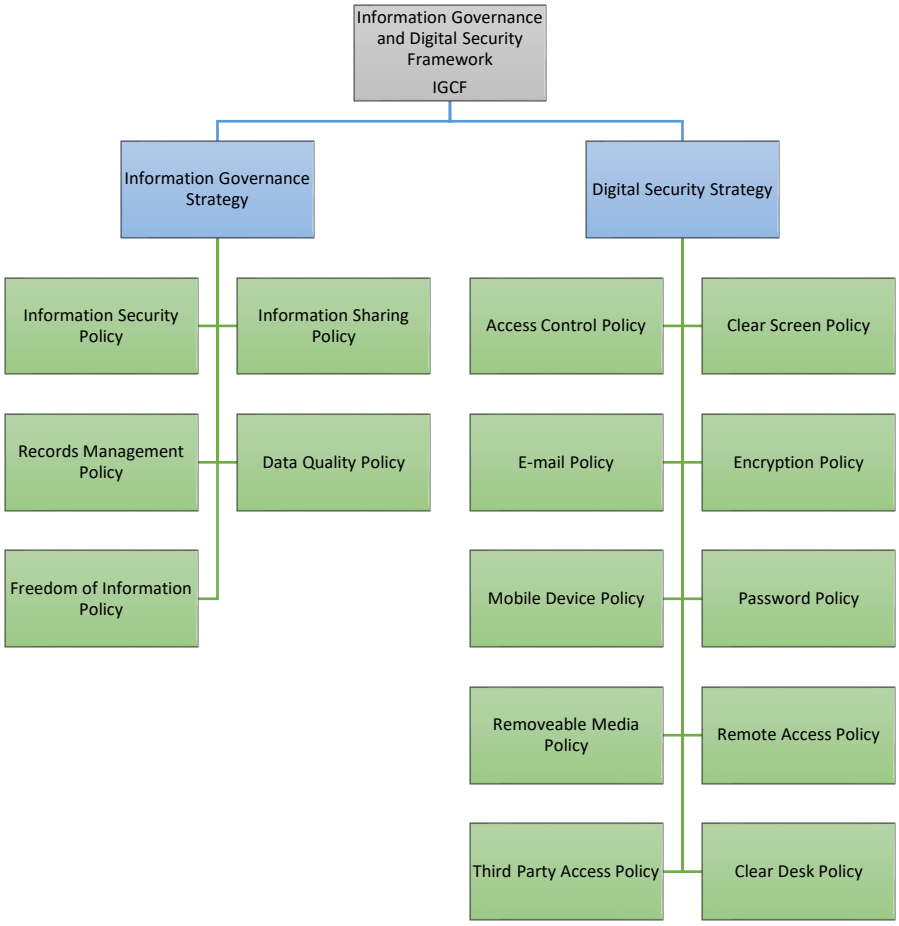
Members are asked to note the Digital Security Framework and associated policies.

- **Awareness** – For Members' information only.

3 List of appendices

The following appendices are included with this report:

- List of Documents and Organogram
- IGDS00 - Digital Security Strategy v1.1
- IGDS01 - Access Control Policy v1.1
- IGDS02 - Clear Screen Policy v1.1
- IGDS03 - E-mail Policy v1.1
- IGDS04 - Encryption Policy v1.1
- IGDS05 - Mobile Device Policy v1.1
- IGDS06 - Password Policy v1.1
- IGDS07 - Removeable Media Policy v1.1
- IGDS08 - Remote Access Policy v1.1
- IGDS09 - Third Party Access Policy v1.1
- IGDS10 - Clear Desk Policy v1.1



IGDS00 - Digital Security Strategy v1.1

IGDS01 - Access Control Policy v1.1

IGDS02 - Clear Screen Policy v1.1

IGDS03 - E-mail Policy v1.1

IGDS04 - Encryption Policy v1.1

IGDS05 - Mobile Device Policy v1.1

IGDS06 - Password Policy v1.1

IGDS07 - Removeable Media Policy v1.1

IGDS08 - Remote Access Policy v1.1

IGDS09 - Third Party Access Policy v1.1

IGDS10 - Clear Desk Policy v1.1

Digital Security Strategy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	Digital Security Strategy		
Document reference number	IGDS00	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

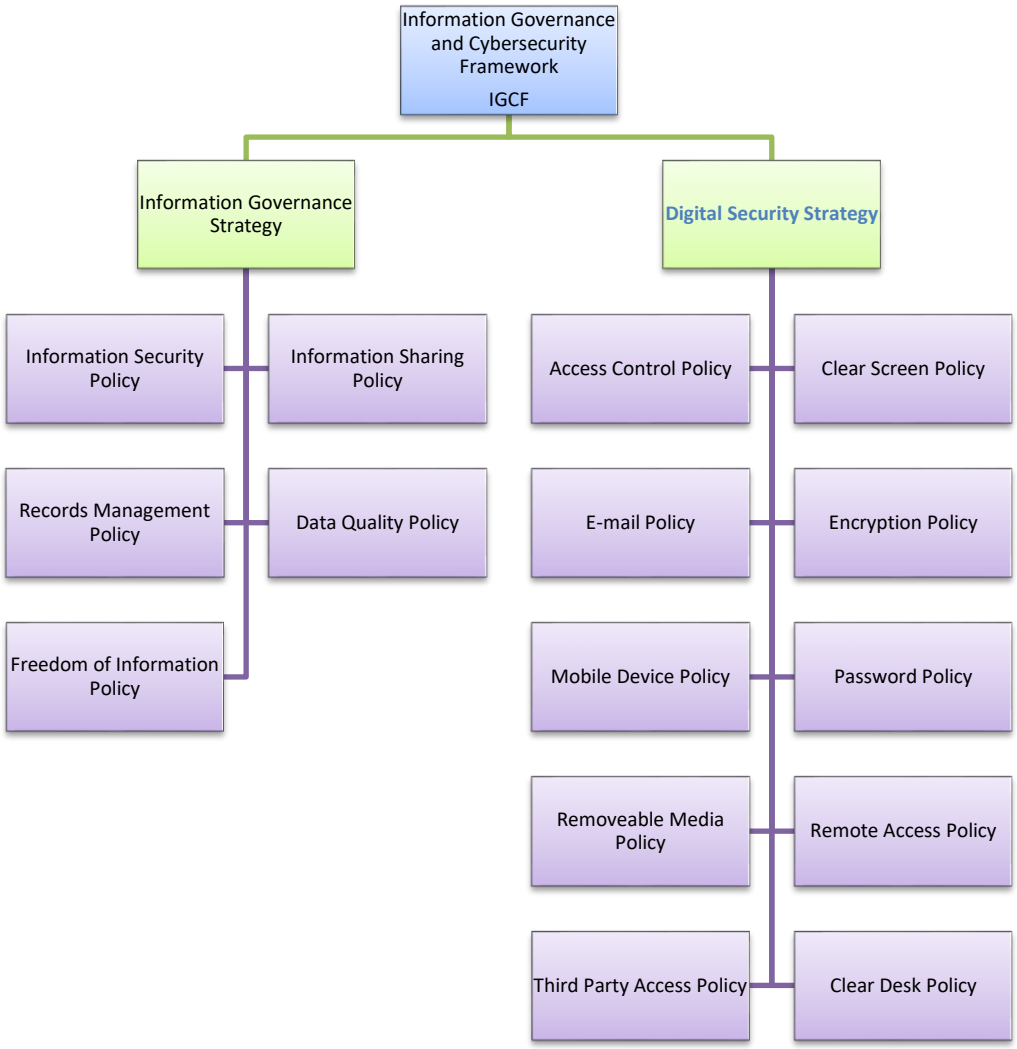
This document sets out the overarching strategy on digital security that NHS Shetland will implement through a suite of policies to preserve the confidentiality, integrity and availability of the information on which its operations depend.

The NHS Shetland Board and senior management are committed to preserving the confidentiality, integrity and availability of all information assets throughout the organisation in order to contribute to the health of the population of Shetland by using data safely and securely ensuring legal, regulatory and contractual compliance.

It is pivotal that NHS Shetland ensures that:

- information risks are identified, managed and treated according to an agreed risk tolerance.
- authorised users can securely access and share information in order to perform their roles.
- physical, procedural and technical controls balance user experience and security.
- contractual and legal obligations relating to information security are met.
- individuals accessing our information are aware of their information security responsibilities.
- adverse events affecting our information assets are resolved, and learnt from to improve our controls.

This strategy forms part of NHS Shetland Information Governance and Cybersecurity Framework (IGCF)



Should staff have any difficulties with understanding any aspect of this strategy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other documents that you may find useful include:

- Information Governance and Digital Security Framework
- Information Governance Strategy
- Individual Information Governance and Digital Security Policies

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner's Office

3. AIM OF THE STRATEGY

The aims of this strategy are:

- to effectively define the risks whether internal or external, accidental or deliberate, relating to the confidentiality, integrity and availability of all types of personal and business information;
- to support the aims and objectives of the overarching NHS Shetland Information Governance and Digital Security Framework;
- to develop a secure technology framework for delivery of the NHS Shetland Clinical Strategy;
- to facilitate secure information sharing between NHS Shetland and other organisations, partnerships and stakeholders;
- to ensure compliance with information security and data protection legislation and the common law obligation to preserve the confidentiality of information;
- to enable a culture of continual improvements in digital security.

NHS Shetland expects the provisions of this strategy to lay the foundation for the alignment of information security practices within the organisation to comply with all legal and regulatory requirements.

4. SCOPE

This document covers all types digital information, including information that is:

- stored electronically on computers, networked servers, cloud services, mobile devices and mobile data storage devices;
- transmitted across a network, including e-mail, telephony, e-mail, collaboration tools, file transfer, application interfaces;

- multimedia including photographs, medical images and scanned documents;
- shared via social media services and available via websites;
- audio and video e.g. digital dictation, video evidence, CCTV

All staff shall meet the standards of practice outlined in this document (and all associated policies) as well as those included within their terms of employment. Those who are registered healthcare professionals must also keep to their own regulatory organisation's standards of conduct and practice.

This strategy and all associated policies and procedures apply to all NHS Shetland staff and contractual third parties with any form of access to NHS Shetland information and or information systems.

This strategy and all associated policies and procedures will be communicated with all staff and other interested parties, and will be revised in line with NSS policy review procedures.

5. INFORMATION SECURITY POLICY PRINCIPLES

- **Confidentiality** - information will be protected to meet regulatory and legislative requirements and all persons covered by this policy will meet these requirements and those set out in the Confidentiality Policy.
- **Integrity** - information will be maintained and robust measures will be taken to prevent the infection of NHS Shetland computers, servers and infrastructure by malicious software, or malware.
    - The latest versions of approved anti-virus programs will be installed on all systems, desktop and laptop computers and updates implemented immediately as they are available.
    - All systems will be updated to the latest identified secure patch or upgrade after these have been assured and tested.
- **Availability** - information will be available where and when a business user requires it in line with their job function.
- Regulatory, contractual and legislative requirements will be met.
- Information asset owners (IAO) will carry out the required information risk assessments:
    - Data Protection Information Assessment (DPIA) and
    - System Security Process (SSP)

  for all IT and data services when:
    - significant changes are proposed to an existing service.
    - prior to implementation of new IT and information systems.
    - a significant information security adverse event has occurred.
- Information will be protected against unauthorised access.
    - Access to all information systems will be controlled to ensure that only authorised users have access to the system and the information they are authorised to access.

- NHS Shetland information systems will have audit functionality which records user access to confidential data items. Audit data will be used for review of actual or potential Information Governance breaches. Routine audit of user access will also be carried out.

- NHS Shetland will put in place arrangements to identify key information assets and their owners and document and maintain these in the Systems Catalogue. Assets will be risk assessed in terms of confidentiality, integrity and availability.
- Business continuity plans will be produced, maintained and regularly tested in order to provide business continuity in the event of information system failure or cyber attack.
- Information security training and awareness materials will be available to all NHS Shetland staff.
- In order to support continuous service improvement NHS Shetland will:
  - ensure that all information security adverse events are reported and managed in line with the Information Security Policy so that lessons learned feed into improvement plans;
  - ensure that where appropriate, adverse events are reported to the appropriate regulatory bodies (e.g. the Information Commissioner's Office, and/or Scottish Government Cyber Resilience Unit).

6. NHS SHETLAND RESPONSIBILITIES

The NHS Shetland Board has accountability for ensuring that NHS Shetland has an Information Security Management System and that adequate controls, assurance and governance is in place.

The NHS Shetland Chief Executive has overall responsibility for managing information risk in a consistent and effective manner, in line with national strategies and NHS Shetland risk appetite, and ensuring that sufficient resources are provided to support the requirements of the policy. The Chief Executive will assign the role of Senior Information Risk Owner (SIRO) at Executive Management Team level, with delegated responsibility for the management of information risk, to oversee the implementation and monitoring of the Information Security Management System and the development of corporate information security objectives.

The SIRO has day to day responsibility for implementing the requirements of all digital information security policy, monitoring compliance and providing the necessary assurance to the NHS Shetland Audit and Clinical Care and Professional Governance Committees. The SIRO will:

- Oversee implementation of this strategy and;
- communicate the above to staff, customers, stakeholders and the wider public to ensure trust is maintained in NHS Shetland digital services across health and social care and other customer data services areas; and
- work closely with members of the NHS Shetland Executive Management Team to ensure that digital information security is supported across NHS Shetland.

The Information and Digital Technology Department has the responsibility to ensure that:

- file servers are housed in secure areas that provide protection from unauthorised access and environmental threats such as fire, flood and loss of power;

- all equipment used to store NHS SHetland data is recorded and any movements tracked to ensure that any theft or loss is detected;
- all information contents are removed before equipment is re-allocated or sent for disposal;
- systematic protection against malware is operated on all computing devices including email gateways;
- data is backed up with offsite resilience, and backups are routinely monitored and tested;
- that connection with third parties is risk assessed and secured.

NHS Shetland Directors are responsible for ensuring that this strategy is implemented consistently in their Directorate.

Line managers are responsible for ensuring that all staff, contractors and other relevant third parties are aware of and follow the requirements of the Digital Security Strategy and its associated policies, to ensure compliance and the necessary safeguarding of information held and maintained by NHS Shetland.

All staff who work for or under contract to NHS Shetland, including contractors, students, agency, bank staff and volunteers are responsible for ensuring that they are aware of and understand the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis, seeking support when necessary.

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a ‘no blame’ culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct

Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. DOCUMENT REVIEW

This strategy will be reviewed every four years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**

Clear Screen Policy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	Clear Screen Policy		
Document reference number	IGDS02	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

NHS Shetland has a responsibility under legislation to ensure that all information and computing devices are held securely at all times including when not in use.

NHS Shetland recognises there is a risk to unauthorised access to systems should computing devices remain unlocked. There is also a potential for sensitive or confidential data to be viewed if left on screen.

This policy forms part of NHS Shetland Information Governance and Cybersecurity Framework (IGCF)

Should staff have any difficulties with understanding any aspect of this policy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other policies / guidelines that you may find useful include:

- Information Governance and Cybersecurity Framework
- Information Governance Policy
- Information Security Policy
- Email Policy

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner's Office

3. AIM OF THE POLICY

The aim for this policy is to establish the minimum requirements for maintaining a "clear screen policy" to make sure confidential/business critical information.

4. SCOPE OF THE POLICY

This policy is applicable to anyone using NHS Shetland IT devices. The terminology included in this policy defines IT devices as any machine that performs calculations automatically - this could include PCs, terminals, and laptops, tablets, smart phones or iPads.

This policy and all associated policies and procedures will be communicated with all staff and other interested parties, and will be revised in line with NHS Shetland policy review procedures.

5. POLICY

A clear screen policy is in effect on NHS Shetland computing device screens. It has been implemented through the deployment of a password-protected screen-saver.

- This is activated automatically on each NHS Shetland managed computing device after a period without user activity of at most 5 minutes. Longer periods have been implemented only where there is a valid reason for doing so.
- Each computing device and multi-function device printer must not be left logged on when unattended and must be protected by key lock, passwords, pass/PIN codes or other controls when not in use.

6. NHS SHETLAND RESPONSIBILITIES

It is the responsibility of all staff to ensure the confidentiality, availability and integrity of data belonging to NHS Shetland, and to comply with the requirements of data protection legislation and Caldicott recommendations. All staff must take personal responsibility for the security of the data in their care.

Line Managers are responsible for ensuring that their staff clearly understand and adhere to this policy.

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a ‘no blame’ culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. POLICY REVIEW

This policy will be reviewed every two years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**

E-mail Policy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	E-mail Policy		
Document reference number	IGDS03	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

NHS Shetland has a responsibility under legislation to ensure that all information and computing devices are held securely at all times including when not in use.

NHS Shwetland business email is based on an Office365 platform which is managed by National Services Scotland (NSS) on behalf of all NHS Scotland organisations.

Users are able to access the services via desktop email applications, Outlook Web Access (OWA) and mobile devices.

E-mail is now part of an integrated suite of tools and applications that are part of the Office365 platform including E-mail, Teams, Planner, Stream and many others.

Care must be taken when using email as a means of communication as all expressions of fact, intention and opinion via email may bind an individual and/or the organisation and can be produced in court in the same way as oral or written statements.

This policy forms part of NHS Shetland Information Governance and Cybersecurity Framework (IGCF)

Should staff have any difficulties with understanding any aspect of this policy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other policies / guidelines that you may find useful include:

- Information Governance and Cybersecurity Framework
- Information Governance Policy
- Information Security Policy
- Email Policy

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner's Office

3. AIM OF THE POLICY

The purpose of this policy is to

- ensure the proper use of the approved NHS Mail service;
- make email users aware of their responsibilities in relation to the management and storage of emails.

4. SCOPE OF THE POLICY

This policy applies to all NHS Shetland staff and contractual third parties with any form of access to NHS Shetland information and or information systems.

This policy and all associated policies and procedures will be communicated with all staff and other interested parties, and will be revised in line with NHS Shetland policy review procedures.

5. POLICY

5.1. General

To maintain security of the email system all email users shall adhere to the following rules:

- NHS Shetland only authorises NHSmail services to be used as business emailing services.
- NHSmail user must comply with the service provider's Acceptable Use Policy.
- Personal email accounts (e.g. Yahoo, Hotmail, Gmail, etc) must not be used for business purposes.
- NSS email accounts shall only be used primarily for NHS Shetland business-related purposes.
- Do not register your NHSmail account for non-business related services (e.g. home delivery services, personal/online shopping, personal social media services, etc.)
- Never use your Network/NHSmail password on any other website or service.
- Do not divulge your email password to anyone. You will never be asked for your email password e.g. by phone or email.
- When leaving your computing device unattended ensure that email is logged out or the equipment is locked to prevent unauthorised access.
- Notify the NHS Shetland Service Desk should you become aware of, or suspect any unauthorised access to, or suspicious activity with your email account.
- Never open a suspicious email. Seek advice from the Service Desk.
- Email should not be used for the long-term data storage of information. Any data shared via email service should be stored to the appropriate network folders.

It is the responsibility of the person sending an email to decide whether email is the most appropriate method to communicate the information. The decision to send an email should be based on a number of factors:

- the subject of the message;
- the recipient's availability;
- the speed of transmission;
- the speed of response required;
- the number of recipients of the email; and the classification ("sensitivity") of the information contained in the email.

When writing a work-related email message it is important that consideration is given to the way in which the message is conveyed including the subject title, text and the addressees. Email messages constitute a formal record and can be used as evidence in legal proceedings.

Staff who have access to email for business purposes may make reasonable personal use of email services. However, personal use of email services should be kept to a minimum and shall not interfere with the performance of staff duties. In addition, it shall not cause additional risk to NSS (e.g. introduction of malware, illegal activities etc.).

Information containing sensitive person identifiable or business information shall be managed in line with data protection legislation and the following guideline.

5.2. Access to another user's mailbox

To manage routine access to another users' or a generic mailbox during routine and planned business absence, these rules must be followed:

- Line managers shall ensure that appropriate business arrangements are in place for the management of an individual's mailbox during their period of absence.
- The owner of a generic mailbox has the responsibility to make arrangements that the generic mailbox is checked during their period of absence.
- Access to the mailbox must be acquired via delegated permissions set up by the owner of the mailbox.
- Passwords must not be shared in order to facilitate access to mailboxes.

To manage non routine access to mailboxes in exceptional circumstances, a request for access will require explicit authority of the relevant Director. Details of the specific access required, and for what purpose will be recorded. Exceptional access is defined by the following scenarios:

- Business continuity e.g. mailbox owner/user is unexpectedly absent (e.g. illness, urgent leave) and key information needs to be retrieved from the mailbox.
- The processing of legislative information requests (e.g. Data Protection, Freedom of Information) in the absence of the mailbox user/owner.
- NHS Shetland investigatory purposes (e.g. evidence of specific behaviours is sought) and it is inappropriate for the mailbox user/owner to search.
- Non-NHS Shetland investigatory purposes (e.g. police investigation) and the mailbox user/owner is unavailable or is inappropriate for involvement in the required search.
- With a court order and when the mailbox user/owner is unavailable or is inappropriate to conduct the required search.

5.3. Housekeeping

It is the responsibility of all users of the service to manage their email messages appropriately. It is important that email messages are managed in order to comply with various statutory obligation as a public authority, such as the Freedom of Information and General Data Protection Regulations, and stored as long only as required in line with *NHS Shetland Records Management Policy*.

6. NHS SHETLAND RESPONSIBILITIES

6.1. All Staff

It is the responsibility of all staff to ensure the confidentiality, availability and integrity of data belonging to NHS Shetland, and to comply with the requirements of the data protection

legislation and Caldicott recommendations. All staff must take personal responsibility for the security of the data in their care.

All staff employed by NHS Shetland or under contract to NHS Shetland, including contractors, students, agency, bank staff and volunteers are responsible for ensuring that they are aware of and understand the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis, seeking support when necessary.

6.2. Line Managers

It is the responsibility of Line Manager to ensure:

- that they and their staff follow this policy.
- they follow NHS Shetland user authorisation procedures.
- they inform the HR when a member of staff joins the organisation, moves or changes their role within the organisation and on termination of employment. This is to enable any remote user access rights to be established, altered and terminated in a prompt manner helping to prevent unauthorised/inappropriate access to data and IT services.

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a ‘no blame’ culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. POLICY REVIEW

This policy will be reviewed every two years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**

Password Policy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	Password Policy		
Document reference number	IGDS06	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

NHS Shetland has a responsibility under legislation to ensure that all information and computing devices are held securely at all times including when not in use.

Passwords are an important aspect of computer and data security. A weak password may result in unauthorised access and/or exploitation of NSS' network infrastructure, data and data services. Passwords are a means of validating a user's identity to access a computer resource, to ensure the security of the resource and to maintain the confidentiality of the information held on that resource. NSS expects its users to select passwords which are secure and to keep all passwords confidential

All users, including contractors and vendors with access to NSS systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This policy forms part of NHS Shetland Information Governance and Cybersecurity Framework (IGCF)

Should staff have any difficulties with understanding any aspect of this policy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other policies / guidelines that you may find useful include:

- Information Governance and Cybersecurity Framework
- Information Governance Policy
- Information Security Policy
- Email Policy

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner's Office

3. AIM OF THE POLICY

The aim of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

4. SCOPE OF THE POLICY

This policy applies to all NHS Shetland staff and contractual third parties with any form of access to NHS Shetland information and or information systems.

It is understood that some legacy systems may not have the capability to meet these stringent password standards. It is however expected of the Information Asset Owner to ensure that where such legacy services exist that they are secured with the maximum password standard

available to the service. Non-compliance with this policy must also be recorded within the individual System Security Policy.

This policy and all associated policies and procedures will be communicated with all staff and other interested parties, and will be revised in line with NHS Shetland policy review procedures.

5. POLICY

5.1. All passwords must conform to the following:

- Passwords must be a minimum of 8 characters long Where available, the minimum password length will be configured in the system, application or service.
- Where available, complex passwords must be used containing the following: upper and lowercase, alphanumeric and special characters Where available, password complexity must be set up within the system, application or service.
- Enforce password history of 12 previously used passwords. Where available, password history must be set up within the system, application or service.
- Passwords must be set to change every 90 days, including a reminder via email that a password change is required (where possible). Where available, password expiration duration and user reminders must be set up within the system, application or service.
- The system, application or service must force a password change on first use of the user account.
- The system, application or service must obscure all passwords entered into the user authentication screen.
- Some technologies/devices such as Smartphone and tablets shall be set to the maximum PIN code length available to that asset (e.g. 4 or 6 digit PIN) with auto-lock (inactivity of the device) set to 5 minutes or less where possible.
- Passwords/PIN codes must be changed when prompted to do so or when the service user suspects their password/PIN code has been compromised.

Users must not use the same password for NHS Shetland accounts and data services as for other non- NHS Shetland access (for example, personal email account, online shopping, etc). Users shall ensure that different passwords are allocated and used on different systems.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.

5.2. Password Storage within user authentication services

All passwords that are stored in any user authentication system/process must be appropriately encrypted to ensure the password can be used as part of the authentication process but not visible to others.

Systems shall be configured to ensure that passwords, if stored, are held in a secure format (i.e. encrypted).

5.3. Passwords in scripts, programs, automated procedures and logins

No passwords shall be incorporated in the hard coding of user accounts in application code.

6. NHS SHETLAND RESPONSIBILITIES

6.1. All Staff

It is the responsibility of all staff to ensure the confidentiality, availability and integrity of data belonging to NHS Shetland, and to comply with the requirements of the data protection legislation and Caldicott recommendations. All staff must take personal responsibility for the security of the data in their care.

All staff are responsible for ensuring that they are aware of and understand the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis, seeking support when necessary.

6.2. Line Managers

It is the responsibility of Line Manager to ensure:

- that they and their staff follow this policy.
- they follow NHS Shetland user authorisation procedures.
- they inform the HR when a member of staff joins the organisation, moves or changes their role within the organisation and on termination of employment. This is to enable user access rights to be established, altered and terminated in a prompt manner helping to prevent unauthorised/inappropriate access to data and IT services.

6.3. NHS Shetland IT system, application and service providers

It is the responsibility of all NHS SHetland IT system, application and service providers to:

- ensure that all user logins are configured to meet the minimum requirements.
- never ask users for their passwords but to ask the user to input their credentials and password for the technical staff.

6.4. Information and Digital Technology Department

The Information and Digital Technology Department has responsibility for the security and use of all service accounts, administrator accounts and third-party access. Any area operating outside of this arrangement may lead NHS Shetland to loss of data, information critical to business processes, or availability of systems.

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a 'no blame' culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. POLICY REVIEW

This policy will be reviewed every two years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**

Removeable Media Policy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	Removeable Media Policy		
Document reference number	IGDS07	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

NHS Shetland has a responsibility under legislation to ensure that all information and computing devices are held securely at all times including when not in use.

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations.

This policy forms part of NHS Shetland Information Governance and Cybersecurity Framework (IGCF)

Should staff have any difficulties with understanding any aspect of this policy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other policies / guidelines that you may find useful include:

- Information Governance and Cybersecurity Framework
- Information Governance Policy
- Information Security Policy
- Email Policy

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner's Office

3. AIM OF THE POLICY

The purpose of this policy is to minimise the risk of loss or exposure of sensitive information maintained by NSS and to reduce the risk of acquiring malware infections on computers operated by NSS.

4. SCOPE OF THE POLICY

- This policy covers all staff in NSS. Removable media means (but is not limited to):
- CDs
- DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers

- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering Machines)

5. POLICY

- The use of removable media shall only be authorised when there is a valid business requirement.
- Only official NHS Shetland approved removable media shall be used.
- Where removable media is allowed to be used it shall be scanned with an approved anti-virus product prior to use.
- Where there is a requirement for data to be burned to CD/DVD or copied to other removable media, this shall have approval of the relevant Information Asset Owner (IAO) for the data, the Data Protection Officer (DPO) or the Senior Information Risk Owner (SIRO).
- The IAO shall consider if there is a requirement to encrypt the data prior to burning to CD/DVD or copying to other removable media. Where the data is personal or confidential then encryption must be utilised.
- The NHS Shetland Information and Digital Technology Department shall ensure all media types are securely disposed of. A request for secure disposal of a removeable media device can be made through the Service Desk portal (link on Intranet).

6. NHS SHETLAND RESPONSIBILITIES

All Staff

It is the responsibility of all staff to ensure the confidentiality, availability and integrity of data belonging to NHS Shetland, and to comply with the requirements of the data protection legislation and Caldicott recommendations. All staff must take personal responsibility for the security of the data in their care.

All staff are responsible for ensuring that they are aware of and understand the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis, seeking support when necessary.

Line Managers

Line managers are responsible for ensuring that all our people and other relevant third parties are aware of and follow the requirements of the policy, to ensure compliance and the necessary safeguarding of information held and maintained by NSS

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a 'no blame' culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. POLICY REVIEW

This policy will be reviewed every two years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**

Remote Access Policy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	Remote Access Policy		
Document reference number	IGDS08	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

NHS Shetland has a responsibility under legislation to ensure that all information and computing devices are held securely at all times including when not in use.

Remote access to NHS Shetland corporate networks is essential to maintain our organisational productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of NHS Shetland, external risks must be mitigated.

These rules and requirements are designed to minimise the potential exposure to NHS Shetland from risks which may result from unauthorised use of NHS Shetland resources. Risks include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical NHS Shetland internal systems, and fines or other financial liabilities incurred as a result of those losses.

This policy forms part of NHS Shetland Information Governance and Cybersecurity Framework (IGCF)

Should staff have any difficulties with understanding any aspect of this policy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other policies / guidelines that you may find useful include:

- Information Governance and Cybersecurity Framework
- Information Governance Policy
- Information Security Policy
- Email Policy

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner's Office

3. AIM OF THE POLICY

The aim of this policy is to define the framework within which NHS Shetland supports the use of Remote Access.

4. SCOPE OF THE POLICY

This policy applies to all NHS Shetland staff and contractual third parties with any form of access to NHS Shetland information and or information systems.

Only NHS Shetland purchased and authorised devices are permitted to be connected to the NHS Shetland corporate network. NHS Shetland devices connecting to this network will be

protected and kept up-to-date with the NHS Shetland authorised security software (e.g. patch management, anti-virus software, etc).

This policy and all associated policies and procedures will be communicated with all staff and other interested parties, and will be revised in line with NHS Shetland policy review procedures.

5. POLICY

- NSS has adopted the NHS Scotland Virtual Private Network (VPN) solution for remote access to the NHS Shetland network via SWAN. NHS Shetland provides two user options:
    - soft token which can be installed on personal/corporate smartphone or;
    - physical token which must generates a one-time access code that changes every time it is used.
- Where a member of staff requires remote access to perform their duties, a request is logged via NHS Shetland Service Portal for approval by the line manager.
- At no time will any NHS Shetland remote access user provide their login credentials to any other individual.
- While using a NHS Shetland owned computer to remotely connect to NHS Shetland's corporate network, authorised users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorised user or third party.
- Staff who use remote access must regularly connect their corporate device(s) to the NHS network directly, in order to ensure all software and security updates have been applied.
- For up to date information regarding NHS Shetland's remote access connection options, consult the Service Desk portal.

6. NHS SHETLAND RESPONSIBILITIES

6.1. All Staff

It is the responsibility of all staff to ensure the confidentiality, availability and integrity of data belonging to NHS Shetland, and to comply with the requirements of the data protection legislation and Caldicott recommendations. All staff must take personal responsibility for the security of the data in their care.

All staff are responsible for ensuring that they are aware of and understand the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis, seeking support when necessary.

6.2. Line Managers

It is the responsibility of Line Manager to ensure:

- that they and their staff follow this policy.
- they follow NHS Shetland user authorisation procedures.

- they inform the HR when a member of staff joins the organisation, moves or changes their role within the organisation and on termination of employment. This is to enable user access rights to be established, altered and terminated in a prompt manner helping to prevent unauthorised/inappropriate access to data and IT services.

6.3. NHS Shetland IT system, application and service providers

It is the responsibility of all NHS Shetland IT system, application and service providers to:

- ensure that all user logins are configured to meet the minimum requirements.
- never ask users for their passwords but to ask the user to input their credentials and password for the technical staff.

6.4. Information and Digital Technology Department

The Information and Digital Technology Department has responsibility for the security and use of all service accounts, administrator accounts and third-party access. Any area operating outside of this arrangement may lead NHS Shetland to loss of data, information critical to business processes, or availability of systems.

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a ‘no blame’ culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. POLICY REVIEW

This policy will be reviewed every two years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**

Third Party Access Policy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	Third Party Access Policy		
Document reference number	IGDS09	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

NHS Shetland has a responsibility under legislation to ensure that all information and computing devices are held securely at all times including when not in use.

In order to provide effective health services, NSS needs to enter into contracts and agreements with outside organisations. For the purposes of this policy, these organisations will be referred to as “third party suppliers”.

The purpose of this policy is:

- to ensure that all contracts and agreements between NHS Shetland and third party suppliers have acceptable levels of information security and information governance processes
- to ensure that personal and sensitive data is protected and managed in line with statutory and good practice requirements

This policy forms part of NHS Shetland Information Governance and Cybersecurity Framework (IGCF)

Should staff have any difficulties with understanding any aspect of this policy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other policies / guidelines that you may find useful include:

- Information Governance and Cybersecurity Framework
- Information Governance Policy
- Information Security Policy
- Email Policy

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner’s Office

3. AIM OF THE POLICY

The aim of this policy is to define the framework within which NHS Shetland supports the use of third party remote access.

It will ensure that all third party organisations that enter into an agreement or contract with NHS Shetland are clear about NSS expectations in terms of information security, governance and confidentiality.

These requirements are designed to minimise the potential exposure to NHS Shetland from risks which may result from unauthorised use of and access to NHS Shetland network infrastructure, physical assets and data.

4. SCOPE OF THE POLICY

This policy applies to all third party organisations or individuals that access NHS Shetland infrastructure either onsite (within an NHS Shetland property) or remotely (outwith an NHS Shetland property), and the NHS Shetland staff who work with these third parties.

This policy and all associated policies and procedures will be communicated with all our people and other interested parties, and will be revised in line with NHS Shetland policy review procedures.

5. POLICY

The overall security of NHS Shetland infrastructure, systems and data takes precedence over any individual requirements for a third party connection.

- A specific business purpose must exist and be defined for a third party connection to be considered. For each third party connection contract, named lead persons responsible for the system and information concerned must be appointed by NHS Shetland and the third party.
- Any third party organisation with which NHS Shetland enters into a service contract that requires third party remote access to NHS Shetland infrastructure must be able to demonstrate compliance with NHS Shetland information security policies and enter into binding agreements that specify the performance to be delivered and the remedies available in the event of non-compliance.
- Third parties permitted access only to NHS Shetland systems and information related to that contract. All other access is prohibited.
- An information security Risk Assessment should be carried out prior to the purchase and implementation of any system.
- A questionnaire should be completed by the third party, in conjunction with the NHS Shetland Sponsor (i.e. the person within NHS Shetland who is requesting the third party access). The questionnaire should be added to the documentation used for the risk assessment.
- Any risks accepted by the sponsoring service owner/Director, could have an impact on the whole organisation (due to NHS Shetland having a single network domain) therefore further consultation and approval by the SIRO might be required.
- Passwords, passphrases, tokens, PINs, Codes and other access controls/authentication methods, should only be supplied to third parties where absolutely essential to enable them to carry out their work on behalf of NHS Shetland as per the agreed contract. These should be revoked or changed once the third party no longer requires them especially at the end of the contract.
- Third parties should also ensure that the operating systems of any devices connected to NHS Shetland network should be patched to an appropriate level, and anti-virus software must be installed and kept up-to-date. In addition, third parties should ensure that only authorised individuals have access to NHS Shetland network.

6. NHS SHETLAND RESPONSIBILITIES

6.1. Head of Information and Digital Technology & Information Asset Owner

It is the responsibility of the Head of Digital and Information Security (HoIDT) and individual Information Asset Owners (IAOs) to ensure that due diligence is followed by making sure that all the information required in the risk assessment process is completed.

6.2. Information Security Team

The team will provide guidance and advice regarding the risk assessment prior to approval by the HoIDT and IAO(s).

6.3. Information Technology Team

The team will review the connection questionnaire and implement appropriate / approved technical controls to mitigate risks.

In the event that a third party connection solution has not been, or cannot be, configured on a specific device then the risks to the information and service shall be assessed and either:

- an alternative access solution shall be utilised for which the risks have been accepted by the relevant NHS Shetland IAO and if required the NHS Shetland SIRO; or
- the existing solution and the risks shall be qualified and accepted by the relevant IAO, and the SIRO. Risks must be added to the risk register.

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a ‘no blame’ culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct

Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. POLICY REVIEW

This policy will be reviewed every two years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**

Clear Desk Policy

Approval date:	**02/11/21**
Version number:	**1.1**
Author:	**Craig Chapman**
Review date:	**02/11/23**
Security classification:	**Not Protected**

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: TBC

NHS Shetland Document Development Coversheet*

Name of document	Clear Screen Policy		
Document reference number	IGDS10	**New or Review?**	**New**
Author	Craig Chapman		
Executive lead	Lorraine Hall		
Review date	02/11/23		
Security classification	Not Protected		

Proposed groups to present document to:		
Information Sub Group (ISG)		
Digital Informatics Support Group (DISG)		
NHS Shetland		

Date	**Version**	**Group**	**Reason**	**Outcome**
01/10/21	0.1	IGSG	PI, PO	PRO
02/11/21	1.0	DISG	PO	A

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)
• For proofing/formatting (PF)	• For upload to Intranet (INT)
• Final Approval (FA)	• Approved (A) or Not Approved, revisions required (NARR)

***To be attached to the document under development/review and presented to the relevant group**

Please record details of any changes made to the document in the table below

Date	Record of changes made to document

Contents

1. SUMMARY

NHS Shetland has a responsibility under legislation to ensure that all business information and assets are held securely at all times including when not in use.

Each user has individual responsibility for ensuring that information in all formats is appropriately secured when their work areas are left unattended and at the end of the day or shift.

This policy forms part of NHS Shetland Information Governance and Digital Security Framework (IGCF)

Should staff have any difficulties with understanding any aspect of this policy or its application, they should discuss this with their Line Manager and if necessary seek further advice from NHS Shetland Information Governance Leads (e.g. Data Protection Officer, Head of Digital, Senior Information Risk Owner)

2. USEFUL INFORMATION

Other policies / guidelines that you may find useful include:

- Information Governance and Digital Security Framework
- Information Governance Policy
- Information Security Policy
- Email Policy

The following external websites may also be of interest:

- NHSScotland Information Security Policy Framework
- Information Commissioner's Office

3. AIM OF THE POLICY

The aim of this policy is to establish the minimum requirements for maintaining a "clear desk policy" to make sure that sensitive/confidential business information is secured in locked areas and out of sight.

4. SCOPE OF THE POLICY

This policy is applicable to anyone working on behalf of NHS Shetland using NHS Shetland systems and handling sensitive/confidential paperwork or mobile data storage/computing devices.

This policy and all associated policies and procedures will be communicated with all staff and other interested parties, and will be revised in line with NHS Shetland policy review procedures.

5. POLICY

NHS Shetland recognises that material left exposed (e.g. on a desk, printer or cupboard top) is more susceptible to damage, disclosure or theft, particularly outside of office hours.

- Sensitive or confidential business information must be locked away (ideally in a fire-resistant safe or cabinet) when not required.
- All removable data storage and portable computing devices (e.g. USB sticks, smartphones, tablets etc.) must be stored in a secure location when not in use.
- Adequate secure storage shall be made available to support the clear desk policy.

6. NHS SHETLAND RESPONSIBILITIES

It is the responsibility of all staff to ensure the confidentiality, availability and integrity of data belonging to NHS Shetland, and to comply with the requirements of data protection legislation and Caldicott recommendations. All staff must take personal responsibility for the security of the data in their care.

Line Managers are responsible for ensuring that their staff clearly understand and adhere to this policy.

7. PERFORMANCE EVALUATION

NHS Shetland will set out the processes for evaluating information security performance. This will include:

- what is to be monitored and how it measured (e.g. security processes, controls and analysis of adverse events);
- standardised methods for evaluation that ensure comparability of measures over time; and
- timescales for carrying out the evaluation and communicating the results to the SIRO.

The SIRO will ensure that actions are taken in response to the evaluations to ensure continuous improvement in information security measures and will report on progress to the NHS Shetland Digital and Informatics Support Group (DISG).

8. FAILURE TO FOLLOW POLICY

Organisational culture is based upon the values of trust, openness, equality and diversity which encourages and supports staff to recognise, report and learn from adverse events. A just culture seeks to learn from organisational/system errors which allow error, whilst ensuring staff do not abdicate responsibilities for their actions. However, a just culture is not a ‘no blame’ culture, so that reckless or malicious behaviour will be challenged and managed through the application of appropriate organisational policies. Whilst it is extremely rare, there may be an occasion where there is evidence that a member of staff has committed a malicious or criminal act. If at any stage in the adverse event review it is deemed that the Management of Employee Conduct Policy should be invoked, HR must be informed so that the disciplinary process can begin. This must not be part of an adverse event review and both processes can run in parallel.

9. POLICY REVIEW

This policy will be reviewed every two years by NHS Shetland and may be reviewed more frequently if new legislation, policies, codes of practice, national standards or changing technologies/systems are introduced.

Date policy is effective: **TBC**