


Department: Public Health	Title: Information Security Policy	
Refer to Other Documents:	Supersedes: v0.2	
Warning -Uncontrolled When Printed The Current Version is Held in The Document Management System		

NHS Western Isles

Information Security Policy



Document Control

Version	Date	Latest changes made by	Status	Reason for change and reviewers
Version 1 Draft 1	08/02/2018	Carol Macdonald	Draft	Reviewed Policy
Version 2 Draft 1	08/07/2020	Maggie Watts	Approved	Caldicott Guardian and Chair of IGSG
Version 2 Draft 2	21/07/2020	Carol Macdonald	Draft	Comments received from CMT July 2020
Version 2 Draft 3	08/09/2020	Jon Harris	Draft	Updated following CEO comments at CMT

Document Approval – Name(s) of the Individual(s) representing the Approving Committee(s)/Group(s)

Reviewers Name	Reviewers Role	Review Date
IGSG	Oversight and Approval	Feb 2018
CMT	Information	May 2018
IGSG	Update to Policy – Oversight and Approval	Jun 2020
CMT	Information	Aug 2020
CMT	Information – with amendments	Sept 2020
Board	Final Approved	28/10/2020

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 2 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

Contents

1	Introduction	4
2	Policy Statement	4
3	Policy	5
3.1	Asset Management.....	5
3.2	Access Control Management.....	6
3.3	Password Management (Windows).....	7
3.4	Boundary Gateways and Firewalls.....	7
3.5	Application Access.....	8
3.6	Monitoring System Access and Use.....	8
3.7	Computer and Network Procedures.....	9
3.8	Personnel Security.....	9
3.9	Protection from Malicious Software.....	9
3.10	Information Security Incidents and Weaknesses.....	10
4	Accountability and Responsibilities	10
5	Legislation	11
6	Education, Training, Monitoring and Reviewing	12

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 3 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

1 Introduction

This IT security policy is a key component of NHS Western Isles overall business management framework and provides the framework for the more detailed information security documentation including system level security policies, security guidance and procedures. Failure to implement effective information security management controls can result in NHS Western Isles becoming exposed to a number of significant threats including (but not limited to):

- Malicious code entering the network;
- Hackers obtaining unauthorised access to systems and data;
- Unauthorised persons gaining access to confidential information;
- Data leakage;
- Compromise of confidentiality, integrity and availability of company sensitive data.

The adverse business impacts potentially flowing from these risks include:

- Loss of availability of key systems and/or loss of data;
- Interruption of normal business operations and resultant loss of revenue;
- Damage to NHS Western Isles reputation and loss of confidence amongst customers, employees, business partners and parent company;
- Allegations of poor corporate governance resulting in adverse publicity and parent company dissatisfaction;
- Confidential business information falling into the hands of competitors and other third parties;
- Reputational damage to NHS Western Isles

Compliance with these policies, procedures and standards is therefore required from all persons who have access to any of NHS Western Isles IT infrastructure or information assets. This includes third parties (e.g. contractors, business partners and – in some cases – customers) as well as employees.

2 Policy Statement

Objectives

The objective of this Information Security Policy is to help preserve the confidentiality, integrity and availability of our business information, based upon a risk assessment and an understanding of our tolerance for risk. The purpose of information security is to ensure business continuity and manage risk by minimising the likelihood and impact of security incidents. Information security enables information to be shared while ensuring the protection of information assets.

Policy Aim

The aim of this policy is to set out the rules governing the secure management of our information assets. It demonstrates Management support for, and commitment to, information security through issuing this policy for user acceptance and compliance, as well as any related policies, procedures and guidelines, including user education and awareness across NHS Western Isles. The purpose of this policy is to protect all NHS Western Isles information assets from threats, internal or external, deliberate or accidental following a risk based approach designed for the:

- prevention of incidents via the identification and reduction of risks;
- detection of incidents before damage can occur;

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 4 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

- recovery from incidents via containment and repair of damage and prevention of reoccurrence.

It will achieve this by ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies; ensuring an approach to security in which all members of staff fully understand their own responsibilities, creating and maintaining within the organisation a level of awareness of the need for information security as an integral part of the day to day business and protecting information assets under the control of NHS Western Isles.

3 Policy

This policy applies to all information, information systems, networks, applications and users of NHS Western Isles or supplied under contract to it.

3.1 Asset Management

Asset Ownership - Each information asset, (hardware, software, application or data) shall have a named owner who shall be responsible for the maintenance of that asset. New Information systems being considered for procurement by NHS Western Isles must include adequate security measures that are clearly documented in the Business Case and defined in the requirements specification. The regulatory framework of the NHS, as well as Data Protection legislation and recommendations of the Caldicott Report must be adhered to throughout the requirement, design and implementation stages. A Privacy Impact Assessment must be completed and approved in advance of any new system, process or software implementation that may impact on data security and/or privacy.

Asset Records and Management - An accurate record of business information assets, including acquisition, ownership, modification and disposal shall be maintained. Sensitive material such as licensed software and sensitive data shall be removed from hardware before disposal.

NHS Western Isles has created an Information Security Management System to capture the Boards Information Assets, identify what information is held, for what purpose, in what format, by whom is it accessed, with whom it is shared and the purpose for sharing. Security measures for each information asset have been identified and each asset risk assessed. This will be accessible to all identified system owners for them to maintain and add to as required.

Removable media - Official removable media shall be provided centrally. Where indicated by a risk assessment, systems should be prevented from using removable media. Use of personal removable media in business information systems (e.g. USB sticks, CD, DVD and personal devices for the purposes of charging etc.) will be prevented, but may be approved by the IT Manager on formal request.

Removable media from external sources - Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the IT Manager before they may be used on business systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

Mobile devices (e.g. phones, tablets, laptops etc.) - All mobile devices including mobile phones, laptops and tablets for use by NHS Western Isles' staff will be provided by the IT

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 5 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

Department. As a result, all devices will be encrypted to the appropriate standard, have up to date firewall and antivirus deployment as standard. Access to mobile devices will be restricted to those who require it for the business needs. NHS Western Isles' IT Department have an up to date inventory of these mobile devices. Users must inform a member of the IT team immediately if the device is lost or stolen and the device must be subsequently completely wiped.

Some systems such as NHS Mail can be accessed through non NHS devices. Such systems would require to be set up and operated in a way compliant with policies applied to other NHS provided systems. Advice on such usage should be sought from NHS Western Isles IT department, and guidance on 'Using Personal Devices while working from Home.' See Appendix A.

If any device used to contain sensitive personal data pertaining to patients, service users or staff which has been lost, stolen or its security compromised must be reported without delay as a Personal Data Breach via Datix. Any loss, destruction, unlawful disclosure of data as a result of a security breach must be reported to the Information Commissioners Office and Scottish Government within 72 hours. This is a mandatory requirement of the 2018 Data Protection Regulation.

Sensitive Information Assets - NHS Western Isles shall identify particularly valuable or sensitive information assets, based upon the ISMS asset type classification. SENSITIVE shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the business or its staff or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the business;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the business in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

A risk based approach to Information Security will aim to meet the following objectives:

- prevention of incidents via the identification and reduction of risks;
- detection of incidents before damage can occur;
- recovery from incidents via containment and repair of damage and prevention of reoccurrence.

3.2 Access Control Management

Physical Access - Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data. It is managers' responsibility to ensure access to sensitive and/or clinical areas is restricted to those requiring it for their roles. Staff are required to contact HR to change or request access with authorisation from line Managers.

User Access - Access to information shall be restricted to authorised users who have a bona-fide business need to access the information. System Access Requests must be

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 6 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

submitted via the Intranet, and authorised by relevant line managers before requests are approved.

- User account requests will be subject to proper justification, provisioning and an approvals process, and assigned to named individuals.
- User account access will be monitored periodically using software to identify accounts that have been inactive for long periods, and access may be revoked if required.
- Authenticate users before granting access to applications or devices, using unique credentials.
- Implement two-factor authentication, where available.
- User accounts will be removed or disabled when no longer required.
- Elevated or special access privileges, such as system administrator accounts, will be restricted to a limited number of authorised individuals and these access privileges will be reviewed at least quarterly.
- Use administrative accounts to perform administrative activities only.
- User activity on clinical systems will be audited in line with Data Protection principles, and users will be asked to provide basic demographics in order to facilitate system audit processes. It is each staff member's responsibility to keep these details up to date.

3.3 Password Management (Windows)

GP sites manage their own windows credentials and due to configuration issues, it is not possible to enforce the same standards as NHS Western Isles.

NHS Western Isles adheres to a strict password policy that must be implemented at all times.

- Passwords must contain a minimum of 8 characters with uppercase and lowercase letters as well as numbers with no maximum length.
- Passwords do NOT need to be changed at regular intervals, however change passwords promptly when the user knows or suspects they have been compromised.
- Passwords are set to be renewed every 90 days.
- Three unsuccessful attempts to log in locks the user account and automatically informs the IT Department.

Using online training materials and at corporate induction, users are advised of the following:

- how to avoid choosing obvious passwords (such as those based on easily-discoverable information like the name of a favourite pet)
- not to choose common passwords - this could be implemented by technical means, using a password blacklist
- how to spot a phishing attack
- not to use the same password anywhere else, at work or at home

Protect against brute-force password guessing, by using at least one of the following methods:

- lock accounts after no more than 3 unsuccessful attempts

3.4 Boundary Gateways and Firewalls

NHS Western Isles maintain boundary security through the use of a firewall, the integrity of this firewall is maintained by adhering to the following rules:

- All default usernames/passwords on boundary devices have been changed and a strong password has been implemented, please see password policy statement.

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 7 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

- All open ports and services on each firewall have been subject to justification and approval by an appropriately qualified and authorised business representative. The business need must be included in the documentation.
- All commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOS, tftp, RPC, rlogin, rsh, rexec) have been disabled or blocked by default at the boundary firewalls.
- All firewall rules that are no longer required are to be removed or disabled in a timely manner.
- Use a host-based firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots
- Domain access to servers has been limited, and accounts are kept separate from all other user accounts.
- All unnecessary remote administrative interfaces have been disabled, unless there is a clear and documented business need and the interface is protected by one of the following controls:
 - a second authentication factor, such as a one-time token
 - an IP whitelist that limits access to a small range of trusted addresses

3.5 Application Access

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access - Where indicated by a risk assessment, hardware should be authenticated by MAC address on the network.

It is not permitted to attach any non NHS issued device to the network without seeking prior permission from the Head of the IT Department.

System Perimeter access - The boundary between the business systems and the Internet or other non-trusted networks shall be protected by a firewall, which shall be configured to meet the threat and continuously monitored.

3.6 Monitoring System Access and Use

NHS Western Isles reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

NHS Western Isles has the ability to monitor user activity in up to 5 clinical information systems through the Fairwarning system. Staff should be fully aware that patterns of system use, suspected misuse or any other perceived unauthorised system use can be monitored, will be reported on as required and action may be taken in line with terms and conditions of employment.

Any breach of IT Security Policy, suspected or confirmed network information security (NIS) breach, suspected or confirmed personal data breach, misuse of clinical system access or deliberate sabotage of NHS Western Isles security network should be reported immediately, and could lead to disciplinary procedures. An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 8 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

3.7 Computer and Network Procedures

Management - Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Head of IT.

Maintenance - Systems hardware, firmware and software shall be updated in accordance with the suppliers' recommendations as approved by the IT Manager.

Patch Management - All software installed on computers and network devices is to be fully licensed and supported by the vendor.

- All security patches and updates are to be applied immediately where possible using our standard change control procedure: where this is not possible this should be noted and included on the department risk register
- Suppliers are expected to comply with ALL local security policy requirements.
- Software must be removed from devices when no longer supported.

Accreditation - NHS Western Isles shall ensure that all new and modified information systems, applications and networks include security provisions, are correctly sized, identify the security requirements, are compatible with existing systems according to an established systems architecture (as required) and are approved by the Head of IT before they commence operation.

System Change Control - Changes to information systems, applications or networks shall be reviewed and approved by the Head of IT and other relevant stakeholders.

Local Data Storage - Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals determined by the business.

External Cloud Services - Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

3.8 Personnel Security

Contracts of Employment – Staff security requirements shall be addressed at the recruitment stage and all prospective staff members shall be subject to a level of security screening appropriate to their role. This shall be conducted by the HR function with advice and input from management as appropriate. As a minimum this should include:

- Verification of identity;
- Employment history (for a minimum of the past three years);
- Verification of nationality and immigration status.

Information security expectations of staff shall be included within appropriate job descriptions and that any breach of information security controls may be considered a misdemeanour under NHS Western Isles disciplinary policy, and which in turn might, under specific circumstances, result in dismissal. All access rights shall be removed immediately on termination of contract.

3.9 Protection from Malicious Software

The business shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 9 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

with this policy. Users shall not install software or other active code on the organisation's property without permission from the Head of IT. Users breaching this requirement may be subject to disciplinary action. It is the responsibility of the IT department to ensure all anti malware software is kept up to date.

All Malware Protection Software will have all engine updates applied, and this application is to be strictly adhered to.

- The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.
- The software must scan web pages automatically when they accessed through a web browser (whether by other software or by the browser itself).
- The software must prevent connections to malicious websites on the Internet (by means of blacklisting, for example) - unless there is a clear, documented business need and the Applicant understands and accepts the associated risk
- Daily Malware scans will be implemented using the company's anti malware software.
- The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily.

3.10 Information Security Incidents and Weaknesses

1. Weaknesses - All breaches of this Policy and other information security incidents or suspected weaknesses are to be reported to the Head of IT immediately. Information security incidents shall be logged without delay on Datix and investigated to establish their cause and impacts with a view to avoiding similar events. If required as a result of an incident, data will be isolated to facilitate forensic examination.
2. Business Continuity and Disaster Recovery Plans - NHS Western Isles shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.
3. Reporting - The IT Manager shall keep the business informed of the information security status by means of exception reporting.

4 Accountability and Responsibilities

Ultimate responsibility for information security rests with the Senior Information Risk Officer (SIRO) who is responsible for ensuring that effective systems, policies and procedures for all systems used to process information in NHS Western Isles are in place.

Information security risk management and operational responsibility will sit with the chair of the Digital Programme Board, chaired by the Nurse Director.

Risks relating to information security should be identified in departmental and divisional risk registers and managed accordingly in line with risk management policy and procedure. The SIRO is ultimately responsible for accepting the residual risks evaluated by the information risk management process (ISMS).

Responsibility for maintaining this Policy, the Information Asset Register and for recommending appropriate risk management measures sits with the Head of IT and the Information Governance Manager. Both the IS Policy and the Asset Register shall be

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 10 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

reviewed annually, or more frequently, if appropriate, by the Information Governance Steering Group (IGSG) with Corporate Management Team oversight.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of, and adhering to:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored. Line managers are responsible for notifying HR and IT about staff who have moved post or left their posts in order for the relevant accounts and accesses to be updated, as required. This includes network access, Paxton badge permissions and system accounts.

Each member of staff shall be responsible for the operational security of the information systems they use taking personal and professional responsibility for dealing securely with any information they have access to in the course of their duties.

Each system user shall ensure that no breaches of Information security result from their personal actions. This is also equally applicable for staff authorised to access and use NHS Western Isles Information systems remotely.

All staff must notify their Line Manager of all suspected or actual breaches of Information security, using the Datix system as required.

Contracts with external parties that allow access to the organisation's information systems shall be in place before access is allowed. These contracts shall aim to ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

NHS Western Isles Information Governance Steering Group will take overall responsibility for Information Security Management which will include representation from:

- IT Security
- Physical Security
- Health Records
- Human Resources
- Risk Management
- The Business via Senior Management.

The IGSG will define ownership and responsibility for Information Governance Policy and Procedures which includes the Information Security policy, within NHS Western Isles. Links to be made with the NHS Western Isles 'working from home' and 'home working' policies, led by HR.

5 Legislation

NHS Western Isles is required to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of NHS Western Isles who may be held personally accountable for any breaches of information security for which they may be held responsible. NHS Western Isles shall comply with the following legislation and other legislation as appropriate:

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 11 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

- The General Data Protection Regulation 2018
- The UK Data Protection Act (UKDPA) 2018
- Network Information Security Regulation (NIS) 2018
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers (Scotland) Act 2000
- Freedom of Information Act (Scotland) 2002
- CEL (2008)45 NHS Scotland Mobile Data Protection Standard
- Copyright, Design and Patents Act 1988
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Privacy and Electronic Communications Regulations 2003 (PECR)

6 Education, Training, Monitoring and Reviewing

Information Security Awareness Training

All staff are made aware of the IT Security Policy in order that they are fully aware of their roles and responsibilities as NHS Western Isles employees. A series of Information Security learning materials will be made available to all staff regularly to ensure staff are IT Security aware.

Information security awareness training shall be included in the staff induction process as part of the Information Governance Corporate Induction training. Users shall be made aware of the procedures applicable to them and refreshed regularly. An on-going awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

With a move to an electronic patient record, and the majority of hospital systems being electronic, in an age of heightened cyber security issues its more crucial than ever to prepare staff in how to spot phishing attacks, identify aspects of social engineering and identify security issues in advance in order to protect clinical services and keep information secure.

Intellectual Property Rights

NHS Western Isles shall ensure that all software is properly licensed and approved by the IT Manager. Individual and NHS Western Isles IPR shall be protected at all times. Users breaching this requirement may be subject to disciplinary action.

Social Media

Social media may be used for business purposes on condition that no sensitive or potentially sensitive material, IP or similar material is disclosed. Users must behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the Managing Director. Users breaching this requirement may be subject to disciplinary action.

NHS Western Isles staff must comply with the Policy on the Personal Use of Social Media by Staff, the Twitter Acceptable Use Procedure, Media Policy and Unauthorised Photography Procedure.

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 12 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

Appendix A

NHS WESTERN ISLES - USING PERSONAL DEVICES WHILE WORKING FROM HOME

In response to the COVID 19 pandemic the rules on the use of personal devices for work purposes has been relaxed however all reasonable steps still need to be taken to keep devices, systems and data secure.

Home working must be authorised in advance by your line manager. If home working means you are using a personal device for work purposes, please consider the following:

Workspace

- Consider the workspace you use at home, the data that you are accessing is confidential and you should ensure that information cannot be viewed or overheard.
- You must not leave an open electronic system whilst away from your desk/workspace.
- Store any printed copies of documents as securely as possible, follow the clear screen and clear desk policy even when working from home. You must not leave confidential data of any sort, printed or otherwise, available to others.

Device Security

- Enable any security features on your device; this could include encryption, two-step verification, passwords, pin numbers or biometric features such as fingerprint or facial recognition.
- Do not use public wifi.
- Ensure your device is fully updated with the latest security updates and patches.
- Laptops and PCs should have anti-virus software installed and be set to automatically update.
- Use the same software and tools that you use in the office rather than downloading other commercial tools.
- Disable message notifications on your device's lock-screen.
- Always take care to ensure you are using the correct NHS Mail account prior to sending an email from a personal device.
- Take care when using a non-work device for sending work related emails, that personal email contacts are not auto completed.

General Advice

- Where possible, do not to mix work and personal activity on your personal device, sharing of personal devices being used for work purposes should be avoided.
- Do not dispose of any sensitive information in a domestic bin, it should be securely disposed of using a personal cross cut shredder or taken in to work premises and placed in confidential waste bags.
- Avoid downloading NHS data particularly where it is of a confidential nature onto personal devices.

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 13 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG

- In situations where NHS data must be downloaded, it should be securely deleted as soon as possible.
- Do not upload NHS data to store or share in commercial cloud storage solutions such as dropbox, googledrive etc. Only NHS Western Isles approved cloud systems should be used.

Follow the latest guidance on recognising phishing emails and other cyber threats. It is your responsibility to be vigilant to fraudulent activity when working from home and or/working using a personal device.

Report any personal data breaches or cyber security breached on Datix immediately or calling the IT Manager via switchboard (01851 704704) or contact IT by emailing wisupport@nhs.net.

Additional advice and guidance is also published on the Information Governance website.

Date Approved: Oct 2020	Review Date: (max 2 yrs.) Oct 2022	Version: 2.3	Author: Carol Macdonald/Jon Harris
Content Approval By & Date: IGSG Jun 2020		Page 14 of 14	Owner: (Director) Dr Maggie Watts
Approval for Use within NHS Western Isles:			Reviewers: IGSG