ACCESS TO NHS HIGHLAND NETWORK AND SYSTEMS POLICY

eHealth Department

Warning – Document uncontrolled when printed

Policy Reference:	1222	**Date of Issue:**	January 2019
Prepared by:	Andrew Nealis	**Date of Review:**	January 2021
Lead Reviewer:	Donald Peterkin	**Version:**	V2.1
Authorised by:	Information Assurance Group	**Date:**	November 2018

Distribution:

All staff

Method:

CD Rom ☐ Email ☐ Paper ☐ Intranet ☒

Version Number	Date	Author	Change summary
V1.0	**January 2014**	**Aileen Fraser**	**Policy published**
V2.0	February 2018	Donald Peterkin	Document Reviewed and updated.
V2.1	December 2018	Andrew Nealis	Updated to reflect changes in data protection legislation

Equality and Diversity Statement

This policy is designed to meet the needs of patients, employees, volunteers and contractors of NHS Highland.

The Equality Act 2010 places a legal obligation on public authorities (including NHS Highland) to actively promote equality in all their work and requires them to ensure that they comply with the general duties to:

- eliminate unlawful discrimination, harassment and victimisation;
- advance equality of opportunity between different groups; and
- Promote good relations between different groups.

The characteristics protected by the equality act are age, disability, sexual orientation, gender reassignment, race/ethnicity, faith and belief, sex, pregnancy and maternity and marriage and civil partnership.

NHS Highland will ensure that it:

- fully meets the needs of potentially disadvantaged individuals or groups;
- has ready access to communication support and other services to support access to NHSH services.

Data Protection Statement

NHS Highland is committed to ensuring all current data protection legislation is complied with when processing data that is classified within the legislation as personal data or special category personal data.

Good data protection practice is embedded in the culture of NHS Highland with all staff required to complete mandatory data protection training in order to understand their data protection responsibilities. All staff are expected to follow the NHS policies, processes and guidelines which have been designed to ensure the confidentiality, integrity and availability of data is assured whenever personal data is handled or processed

The NHS Highland fair processing notice contains full detail of how and why we process personal data and can be found by clicking on the following link to the 'Your Rights' section of the NHS Highland internet site.
http://www.nhshighland.scot.nhs.uk/Pages/YourRights.aspx

1. INTRODUCTION

The NHS Highland eHealth Department receives and processes numerous requests for network and system access which results in the issue of usernames and passwords. A proportion of these requests are for staff not employed by NHS Highland.

The NHS Scotland Information Security Policy Framework requires that access to NHS networks and systems must be strictly controlled as does the requirements of the EU General Data Protection Regulations (GDPR) and the Network, Information System (NIS) directive and Network and Information Systems (NIS) Regulations 2018. It is acknowledged and recognised that in certain circumstances there are potential risks associated with refusing access when there is a sound and demonstrable reason for that access.

This policy has been developed to ensure a consistent, but flexible, approach to all access requests whilst maintaining the requirement that User Access Management for a third party should normally be based on formal employment contracts which include all the necessary security conditions to satisfy the NHS Highland security requirements.

2. OBJECTIVES

The following points outline the objectives of this document:

- to preserve the confidentiality, integrity and availability of data within NHS Highland;
- to provide management direction and support for information security and access;
- to ensure security is an integral part of working with information (whether manual or electronic);
- to ensure there is compliance with relevant legislation relating to the collection, maintenance and protection of information, access to information (whether manual or electronic) is on a strictly need to know basis;

3. LOCATION

This Policy is applicable to all staff, contractors and volunteers requiring access to NHS Highland Network and Systems.

4. RESPONSIBILITY

4.1. Chief executive

The final responsibility for the secure access and operation of all systems used by NHS Highland is vested in the Chief Executive. This responsibility is delegated to Line Managers and the head of eHealth and ultimately staff (via the directorate structure).

4.2. Caldicott Guardian

The Caldicott Guardian is the senior person responsible for ensuring NHS Highland is adequately protecting the confidentiality of people's health and care information and making sure it is used properly

4.3. Senior Information Risk Owner (SIRO)

The SIROs role in the organisation is to lead and foster a culture that values, protects and uses information for the success of the organisation and benefit of its patients.
The SIRO provides Board level accountability that information risks are identified and managed in accordance with the NHS Highland risk appetite.
The SIRO s focus is on the impact of information risks on the delivery of business objectives rather than viewing information risks from a technical perspective.

4.4. Information Assurance and IT Security Team

The Information Assurance & IT Security Team for NHS Highland is responsible for the implementation and enforcement of this policy and will;

- Maintain an oversight of access arrangements
- Risk assess new requests for access that fall out with routine business
- Administer Clinical Signatory list

4.5. eHealth Department

The eHealth department has responsibility to;

- Administer requests for access
- Review and amend access permissions
- Remove or suspend access no longer required
- Monitor use of IT systems
- Audit access to IT systems

4.6. Line Managers

Managers have responsibility to;

- Ensure staff have appropriate access for their role on commencing employment with NHS Highland
- Notify eHealth Service desk of any staff changes that may affect access rights (eg change in role, changing/ leaving department or NHS Highland) so that accounts can be amended or disabled as appropriate
- Ensure that current and future staff have completed training in Safe information Handling
- Ensure that staff have received appropriate training specific to their role on the use of NHS Highland IT systems.
- Managers will ensure that no unauthorised staff are allowed to access any of the organisations computer systems as such access could compromise data integrity.

4.7. All Staff, Contractors and Volunteers

All members of NHS Highland staff, contractors, volunteers and service providers who require access to the use of NHS Highland IT systems must conform to the standards expected and described in this policy statement and associated NHS Highland Policies
All staff must complete statutory and mandatory training in relation to Safe Information Handling. Contractors and volunteers must sign the appropriate confidentiality agreements, Appendix 1.

5. AUTMATIC ACCESS TO NHS HIGHLANDS NETWORK AND SYSTEMS

All NHS Highland staff will be entitled to access to NHS Highland's network and systems, commensurate to their role, on beginning employment with NHSH.

The following groups of persons are eligible for controlled and auditable network logins and access to such systems as are required for the job:

- NHS Highland Employees including Agency Locums
- Short Term Employees (Temps)
- Board Members

- Honorary Contract Holders
- Research Passport Holders

6. STUDENTS

The following student groups are eligible for network logins and access to such systems as are required for the job:

- Medical
- Nursing
- Dental
- Allied Health Professionals
- Administration and Clerical

The Head of Department in which they are working within should sponsor them. This may be via the Medical Staffing Department or from the discipline specific department e.g. Physiotherapy. Work placement students will be considered on a case by case basis.

7. JOINT WORKERS

NHS Highland has many joint teams such as the Community Mental Health Teams which consist of NHS and Local Authority staff. Only NHS staff can automatically obtain access to NHS Highland's network. However, as part of joint working and the integration process some Local Authority staff may require to access the same file structure or system as the rest of the team. Access will be provided on completion of the appropriate application form which has been approved by the Joint Worker's line manager in accordance with the Joint Workers' Agreement. Where no Joint Workers' Agreement exists access will be considered on a case by case basis.

8. 3rd PARTY CONTRACTORS

The following groups of persons are eligible for network logins and access to such systems as are required for the job:

- ATOS ORIGIN ALLIANCE
- SUPPLIERS OF SERVICES TO NHS HIGHLAND

The prerequisites are that they have signed the confidentiality agreement with NHS Highland as well as the 3rd party contractor's statement (Appendix 1). The NHS Highland eHealth Department will control the appropriate access. N3 Code of Connection or Statement of Compliance as per N3's guidance must also be in place in respect of network connectivity.

There may be some exceptions to the above eg. When a contractor requires access to NHS Highland's network and is physically on site. The Head of eHealth or Head of eHealth Infrastructure Services will decide if access should be granted in these circumstances. Access will be set to expire at the end of the on-site requirement.

9. PATIENT ACCESS

This policy does not allow access to NHS Highland's Network and Systems for patients. The exception to this rule is when patients who require access to an application or the internet for clinical purposes. This must be done under clinical supervision with appropriate security e.g.

restricted profiles and these will be provided via the NHS Highland eHealth Department on a case by case basis.

8. TRAINING AND RESEARCH

If access to the network and systems is for training or research then patients must freely give their specific, informed and explicit consent before the individual accesses any patient identifiable data. Permission of the Caldicott Guardian is required where training and research uses patient identifiable data.

10. OTHER ACCESS TO NHS HIGHLAND NETWORK SERVICES

Should any other access to NHS Highland network services be requested, the prerequisites are that they have produced a business requirement for such access. The individuals should also have made themselves familiar with the NHS Scotland Code of Practice on Protecting Patient Confidentiality and signed the confidentiality agreement with NHS Highland. This is the responsibility of the requestor of the access request. Both the Information Assurance & IT Security Team and the Head of eHealth Infrastructure Services will have to authorise any such request.

11. COMPLIANCE

NHS Highland will comply with all relevant legislation and give consideration to advisory instructions from NHS Scotland and central Government bodies

NHS Highland will respect the license conditions and intellectual property rights of software manufacturers. It will maintain a record of requests and administration of staff access to IT systems.

All members of NHS Highland staff, contractors, volunteers and service providers who require access to the use of NHS Highland IT systems will comply with all relevant legislation. This includes but is not limited to The Human Rights Act 1998, Common Law Duty of Confidentiality, Misuse of Computers Act 1990 and the appropriate Data Protection Legislation.

12. Related Documents

NHS Highland Information Security Policy
NHS Highland Information Governance Policy
NHS Highland Data Protection Policy

13. References

Computer Misuse Act 1990
Data Protection Act 2018
EU General Data Protection Regulations
Human Rights Act 1998
Freedom of Information (Scotland) Act 2002
NHS Scotland Information Security Policy Framework July 2015
Network & Information Systems Directive
Network & Information Systems Regulations 2018

Appendix 1

NHS Highland

Raigmore Hospital
Old Perth Road
Inverness, IV2 3UJ
Telephone: 01463 704000
www.nhshighland.scot.nhs.uk

Third Party Confidentiality, Data Protection and Caldicott Statement for Access to Patient or Board Information

Whilst providing a service for the NHS Highland (the Board) you are likely to have access to personal information in various formats, including verbal, paper and electronic records.
Access to all of this information is governed by data protection legislation and NHS regulations.

All information must at all times be viewed in accordance with the principles laid down in the Data Protection Act 2018.
You are required to keep any data you may need to access confidential, irrespective of the format in which it was obtained. This includes data relating to members of Board staff, patients, relatives and friends who are or who may become patients of the Board and any other personal or commercially sensitive information. Particular care should be taken in telephone conversations and electronic communications, all of which should be conducted in a confidential manner. It is strictly forbidden for you to look at any information relating to yourself, your family, friends, colleagues or acquaintances. Any breach of confidentiality will result in the removal of your access to all Board systems and locations, and in the event of serious breach could lead to criminal prosecution.

Confidential information must not be disclosed to other parties without prior authorisation from the Board.
Declaration
We understand that during the course of our support of NHS Highland, we may come into contact with information of a confidential nature concerning patients, prospective patients, or other Board-owned information. By signing this form we undertake:

- To safeguard adequately any information that we come across in the course of supporting the Board;
- NOT to make copies of or store any Board owned or patient information without the written permission of the Board eHealth Department. In any event, any copies made must be returned to the Board upon request;
- To erase securely all consequential documents created by us from our computer systems or storage media at the end of the assignment;
- NOT to disclose or discuss information concerning current, former or prospective patients with unauthorised parties;
- NOT to retain, disclose, copy, share, reproduce or otherwise to make use of any Board-owned information or material without prior Board authorisation, or to utilise such information in an inappropriate manner;
- That any access to internet services made available through the Board's network will only be used for troubleshooting purposes, or for the downloading of files required to support the Board.

If there are any doubts when dealing with a particular enquiry, reference should be made to the Board eHealth Department.
We acknowledge that this is the only declaration we are required to sign regarding patient or Board confidentiality, and this declaration will be extended to include any subsequent contact with the Board.

We understand that we are responsible for the security of any electronic system username and password issued to us and that this will only be disclosed to relevant people involved in supporting the Board.

We undertake never to attempt to access electronic patient information by using any other password other than that issued specifically for the purpose of supporting the Board, or by other unauthorised means.

If we have reason to believe that the confidentiality of our password has been broken, we will report this to the Board eHealth Department immediately.

Signed:	
Name:	
On behalf of (company):	
Job Title:	
Date:	