NETWORK SECURITY POLICY

Chevin medical

Version:	1
Ratified by:	
Date ratified:	
Name & Title of originator/author:	Steve Creighton, Senior Information Governance Officer
Name of responsible committee/individual:	
Date issued:	2019
Review date:	2020
Target audience:	All staff

Equality Statement

This policy applies to all employees, Managing Partnership members and members of Chevin irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. INTRODUCTION

This Network Security Policy sets out the Practice's overall approach to the maintenance of the integrity, confidentiality and availability of its information technology infrastructure and sets out the responsibilities for ensuring compliance with this guidance.

The policy forms part of the overall Practice approach to information governance and should be read in conjunction with the organisation's other information governance and security policies and procedures.

2. AIMS

The aim of this policy is to ensure that all staff understand their obligations with regard to the network infrastructure and the acceptable use of information technology equipment and systems which they come into contact with in the course of their work. It also provides assurance to the Managing Partnership that such systems are maintained and used legally, securely, efficiently and effectively.

The Practice will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the GDPR/Data Protection Act 2018, records management guidance, information security guidance, other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Security Protection Toolkit.

Application of the policy will ensure the networks used by the Practice:

- Are available when and where required
- Are secure at all times
- Retain their integrity
- Are protected from unauthorised or accidental modification
- Are designed and maintained to preserve confidentiality
- Protect information assets

3. SCOPE

This policy must be followed by all staff who work for or on behalf of the Practice including those on temporary or honorary contracts, secondments, volunteers, pool staff, Board members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Practice. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy applies to:

All networks to which the organisation has access for:

- The storage and sharing and transmission of clinical data and images
- The storage and sharing and transmission of non-clinical data and images
- Printing or scanning clinical or non-clinical data and images
- The provision of Internet systems for receiving, sending and storing clinical or non-clinical data and images
- The provision of remote access to internal systems via secure access routes

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

4. ACCOUNTABILITY AND RESPONSIBILTIES

There are a number of key information governance roles and responsibilities that the Practice need to have in place as part of its Information Governance Framework, these are:

- DPO
- Managing Partnership
- Governance, Performance and Risk Committees
- Caldicott Guardian
- Information Asset Owners/Administrators
- Heads of Service/department
- All employees

In addition to the responsibilities outlined in this policy all individuals must ensure through their normal working practices that the network is protected through such safeguards as locking screens when not in use, logging off the network when finished, prevent the introduction of malicious software.

4.1 Provision of IT and Network Services

Some IT and network services are provided by a service provider contracted by the CCG on behalf of the Practice. The service provider has provided assurances to the Practice to ensure the integrity, confidentiality and security of Practice information in the provision of those services. Therefore, some of the roles and responsibilities outlined in this policy refer to staff roles that are part of the service provider organisation e.g. Head of Information Technology who will have specific responsibilities in terms of ensuring process and security arrangements are complied with. However, the overarching responsibility for security of Practice information affected by the operation of the network remains with the Practice.

5. DEFINITION OF TERMS

The words used in this policy are used in their ordinary sense and technical terms have been minimised.

The network is a collection of communication equipment such as servers, computers, printers, switches, hubs and routers, which have been connected together. The network is created to share data, software, and peripherals such as printers, photocopiers, Internet connections, email connections, tape drives, hard disks and other data storage equipment.

6. PROCESSES FOR ENSURING NETWORK SECURITY

Some of the roles and responsibilities mentioned below will be of staff who are employees of the service provider organisation who provide IT services, these include Head of Information Technology (IT), Chief Information Officer, Network Manager and Information Security Manager.

6.1 Physical and Environmental Security

- Access to secure areas housing critical or sensitive network equipment should be restricted to those whose job requires it. .
- Network computer equipment will be housed in a controlled and secure environment.
- Critical or sensitive network equipment will be protected from power supply failures by the use of Uninterruptible Power Supply (UPS) devices**.**
- Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
- All visitors to secure network areas must be made aware of network security requirements.
- All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
- The Head of IT or Network Support Manager will ensure that all relevant staff are made aware of procedures for visitors and those visitors are escorted, when necessary.

6.2 Access Control to the Network

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- Where remote access to the network is implemented remote access policy and procedures.
- There is a formal, documented user registration and de-registration procedure for access to the network.
- The staff member’s Line Manager of the user must approve the application.
- Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- Security privileges (i.e. 'super user' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis.

- Access will not be granted until the Network Support Manager, IT Helpdesk, or Head of IT registers a user.
- All users to the network should have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret.
- User access rights will be immediately removed or reviewed for those users who have left the organisation or changed jobs.

6.3 Third Party Access Control to the Network

Third party access to the network will be based on a formal contract that includes a standard clause which satisfies all necessary NHS confidentiality and security conditions , and all third party access to the network must be logged.

6.4 External Network Connections

- All connections to external networks and systems must have documented and approved system security policies and procedures.
- All connections to external networks and systems must conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance
- All external connections must be approved by the Information Security Manager.

6.5 Connecting Devices to the Practice Network

- All devices connected to the Practice network are governed by the NHS Statement of Compliance.
- The connection of any equipment to the Practice network requires authorisation from the IT service provider.
- All electronic processing devices connecting to the Practice network must be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that the anti-virus software is up to date.
- Personally owned devices should only be directly connected to the Network with appropriate authorisation from the IT service provider. ‘Personally owned’ refers to devices that are not provided by the Practice or other NHS organisation and directly connected means either by network cable or corporate Wi-Fi. However, a guest Wi-Fi facility can be used.
- The Practice has the facility to allow non-NHS provided devices to connect to the internet via a ‘guest’ wireless connection. This will be via password that is changed regularly.
- External visitors may connect to the internet via a ‘guest’ Wi-Fi account.

6.6 Maintenance Contracts

The CCG currently manage maintenance contracts and periodically review them for all network equipment.

6.7 Fault Logging

Practices are responsible to logging any fault via the IT service provider in question.

6.8 Network Operating Procedures

Documented operating procedures should be prepared for the operation of the network, to ensure its correct, secure operation. Changes to operating procedures must be authorised by the IT Lead.

6.9 Data Backup and Restoration

- Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all relevant technical staff.
- Any backup tapes will be stored securely..
- Users are responsible for ensuring that they back up their own work-related data to the network server i.e. not storing data on a local hard drive.

6.10 Malicious Software

Measures are in place to detect and protect the network from viruses, malware, ransomware and other cyber threats.

6.11 Unauthorised Software

Required use of any non-standard software equipment processing Practice information must be notified to the IT Lead before installation. All software used on NHS equipment must have a valid licence agreement. It is the responsibility of the “owner” or responsible user of non-standard software to ensure that this is the case.

Any new additional PCs added to the network must have a licence for the appropriate software i.e. Operating System, Clinical System, Exchange Client, Anti-Virus, Microsoft Office etc.

6.12 Changes to the Network

- Any proposed changes to the network will be reviewed and approved by the Head of IT
- The Head of IT may require checks on, or an assessment of the actual implementation based on the proposed changes.
- The Head of IT is responsible for ensuring that selected hardware or software meets agreed security standards.

6.13 Security Monitoring

The Head of IT will ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

6.14 Reporting Security Incidents and Weaknesses

A major incident would constitute a loss of function of a system or breach of confidential information for one or more individuals or a breach of information which is likely to lead to harm to an individual, therefore:

- All potential security breaches must be reported in accordance with the requirements of the Incident Reporting Policies.
- Investigations will be undertaken by the appropriate Information Technology Officers or someone nominated by them.
- Incidents will be reviewed in line with the Incident Reporting Policies.
- For any information governance related incident, especially related to a breach of the GDPR/Data Protection Act 2018 such as one that has the potential to be classed as Information Governance and Cyber Security Serious Incidents Requiring Investigation, this will need to be logged on the Incident Reporting Module on the Data Security and Protection Toolkit to grade the incident. The Practice Toolkit Administrator will have access to the module and can grant access to appropriate staff. Examples of SIRIs are when there is a loss of personal data involving many individuals or where particularly sensitive personal information is lost or sent to the wrong address. Staff must read the Incident Reporting Policy for general reporting of incidents and the process for SIRIs.

7. TRAINING

Information governance and security will be a part of induction training and is mandatory for all staff. The Practice will identify the information governance training needs of key staff groups is specified in the IG Training Strategy, which taking into account their roles, responsibilities and accountability levels and will review this regularly through the Personal Development Review processes.
It is a line management responsibility to ensure that all staff are made aware of their information security responsibilities through generic and specific staff training.

8. IMPLEMENTATION AND DISSEMINATION

Following ratification this policy will be disseminated to staff via the Practice's Intranet and/or communication through in-house staff briefings or via email

This Policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

9. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the Date Security and Protection Toolkit (DSP)will be undertaken each year- this includes Confidentiality and Data Protection. All serious information governance incidents must be reported..

10. ADVICE

Advice and guidance on any matters stemming from the policy can be obtained by contacting your line manager

11. ASSOCIATED DOCUMENTS (Policies, protocols and procedures)

The Practice will produce appropriate procedures and guidance in conjunction This will include an Information Governance Handbook which will be updated annually and which will be given to all staff.

This policy should be read in conjunction with:

- Confidentiality and Data Protection Policy
- Records Management and Information Lifecycle Policy
- Freedom of Information and EIR Policy
- Information Governance Strategy
- Information Governance Policy and Management Framework
- Information Security Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Policy

And their associated procedures (including but not limited to)

- Access to Records Procedure
- Information Sharing Protocol
- Freedom of Information Procedures
- E mail and Internet Procedures
- Privacy Impact Assessment procedure
- Remote Access and Home Working Procedures
- Safe Transfer Guidelines and Procedure
- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Internet and Email Policies and Procedures
- Any system specific procedures

12. LEGAL REFERENCES AND GUIDANCE

- NHS Act 2006

- GDPR/Data Protection Act 2018
- Human Rights Act 1998
- Computer Misuse Act 1990
- Caldicott Guidance
- Common Law Duty of Confidentiality
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 2018)
- Health and Social Care Act 2012
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Privacy and Electronic Communications Regulations 2003
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- NHS Information Security Management Code of Practice 2007
- ISO/IEC 27001:2005 Specification for an Information Security Management system
- Health and Social Care Information Centre Guidance
- Professional Codes of Conduct and Guidance
- Information Commissioner’s Guidance Documents