Network Security Policy	
Author	Kath Allen Information Governance Specialist (NHS Leeds CCG), David Green Information Governance Advisor (NHS Leeds CCG),Simon Boycott Head of Development and Governance
Corporate Lead	Chief Executive / Senior Information Risk Owner
Document Version	1.0
Document Status	DRAFT
Date approved by Quality, Performance & Finance Committee	
Date issued	
Review date	

Executive Summary

This document defines the computer network security policy for the Leeds General Practice Confederation and this policy applies to all business functions, staff and information contained on the network, the physical environment and relevant people who support the network.

It sets out the policy for the protection of the confidentiality, integrity and availability of the network as well as security responsibilities for ensuring the security of our networks.

The network for the purpose of this policy is a collection of communication equipment such as servers, computers and printers which are connected together using our local and wide area networks.

NETWORK SECURITY POLICY

1. INTRODUCTION

This Network Security Policy sets out the Leeds GP Confederation (Confederation) 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 Confederation 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 Executive that such systems are maintained and used legally, securely, efficiently and effectively.

The Confederation will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of Data Protection Act 1998, records management guidance, information security guidance, other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Information Governance Toolkit. The Toolkit standards are:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance

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

- 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 Confederation including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Confederation. 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 non-clinical data and images
- The storage and sharing and transmission of clinical data and images
- Printing or scanning non-clinical or clinical data and images
- The provision of Internet systems for receiving, sending and storing non clinical or 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 RESPONSIBILITIES

There are a number of key Information Governance roles and bodies that the Confederation needs to have in place as part of its Information Governance Framework, these are:

- Strategic Board
- Executive
- Quality, Performance and Finance Committee
- Accountable Officer
- Senior Information Risk Owner
- Caldicott Guardian
- Information Asset Owner
- Heads of Service
- All employees

The accountability and responsibilities are set out in more detail in the Information Governance Policy and Framework which must be read in conjunction with this policy.

In addition to responsibilities outlined in the Information Governance Policy and Framework some additional responsibilities are detailed in respect of network security for employees. They 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. These safeguards are covered within the sections of this policy and also in the **Information Handling Policy** which details safeguards in the workplace.

4.1 Provision of IT and Network Services

IT and network services are provided by NHS Leeds CCG on behalf of the Confederation. The CCG will work within it's policies and standard operating procedures to ensure integrity, confidentiality and security of Confederation 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 Confederation information affected by the operation of the network remains with the Confederation.

5. DEFINITION OF TERMS

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

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 CCG who provide IT services, these include Head of Information Technology (IT), Chief Information Officer, Network Manager and Information Security Manager.

6.1 Risk Management

- Risk assessments will be carried out in relation to all the business processes covered by this policy as part of business continuity and disaster recovery planning. These risk assessments will cover all aspects of the network that are used to support business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

- Risk assessments will be conducted by the CCG to ensure the networks conforms to ISO27001

- Risk assessments will be conducted by the CCG to determine the Information Technology Security Evaluation Criteria (ITSEC) Assurance levels required for security barriers that protect the network.

6.2 Physical and Environmental Security

- Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The Head of IT will maintain and periodically review a list of those with unsupervised access.
- Network computer equipment will be housed in a controlled and secure environment.
- Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
- The Head of IT is responsible for ensuring that door lock codes for entry to

Network Equipment are changed periodically where there has been a compromise of the code, it is suspected that the code has been compromised, or when required to do so by the Chief Information Officer.

- 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 authorised by the Head of IT or the relevant Network Support Manager for that area.
- 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 that visitors are escorted, when necessary.

6.3 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 home working/mobile working procedures will apply.
- There is a formal, documented user registration and de-registration procedure for access to the network. Forms for new user, changes and leavers are available on the CCG Extranet.
- The staff member's line manager 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 will 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.

6.4 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 completion of A New User Form must also be completed and all third party access to the network must be logged.

6.5 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.

6.6 Connecting devices to the Confederation Network

- All devices connected to the Confederation network are governed by the NHS Statement of Compliance.
- The connection of any equipment to the Confederation network requires authorisation from the IT service provider.
- All electronic processing devices connecting to the Confederation 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 Confederation 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 Confederation 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 the publicly available 'NHS Wifi' SSID.

6.7 Maintenance Contracts

The Network Support Manager/Head of IT will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Asset Register.

6.8 Fault Logging

The Head of IT and Help Desk Manager are responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

6.9 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 Head of IT.

6.10 Data Backup and Restoration

- The Network Support Manager and their team are responsible for ensuring that backup copies of network configuration data are taken regularly.
- Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all relevant technical staff.
- All backup tapes will be stored securely and a copy will be stored off-site.
- Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
- 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.

6.11 Malicious Software

Measures are in place to detect and protect the network from viruses and other malicious software – viruses, spyware, Trojan horses, worms etc.

6.12 Unauthorised Software

Required use of any non-standard software equipment processing Confederation information must be notified to the Head of IT 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

Software is no longer centrally funded from a National Programme. Any new additional PCs added to the network must have a licence for the appropriate software i.e. Operating System, SQL Client, Exchange Client, Anti-Virus, Microsoft Office etc.

6.13 Changes to the Network

- Any proposed changes to the network will be reviewed and approved by the Head of IT and passed where appropriate to the Chief Technology Officer. The Network Support Managers are responsible for updating all relevant design documentation, security operating procedures and network operating procedures.
- The Head of IT or the Chief Technology Officer 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.
- As part of acceptance testing of all new network systems, the Head of IT will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.
- Testing facilities will be used for all new network systems. Development and operational facilities will be separated.

6.14 Security Monitoring

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

6.15 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 and the SIRO must be informed about serious incidents.

- 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

- Any information governance related incident, especially related to a breach of the Data Protection Act such as one that has the potential to be classed as a Serious Incident Requiring Investigation (SIRI) will need to be logged on the Incident Reporting Module on the Information Governance Toolkit to grade the incident. The Confederation Information 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 Confederation will identify the information governance training needs of key staff groups taking into account their role, responsibility and accountability levels and will review this regularly through the Training Needs Assessment process.

8. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Quality, Performance and Finance Committee this policy will be disseminated to staff via the Confederation's website and communication through in-house staff briefings.

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 Data Security and Protection Toolkit (DSP), will be undertaken each year. This includes information and network Security, confidentiality and data protection. Incidents are reported and all serious information governance issues must be reported by the SIRO at Executive level and in Annual Reports.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity by contacting the Confederation Counter Fraud Specialist at the following link: Counter fraud

10. ADVICE

Advice and guidance on any matters stemming from the Policy can be obtained by contacting:

yhcs.infogov@nhs.net

11. ASSOCIATED DOCUMENTS(Policies, protocols and procedures)

The Confederation 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 code of Practice
- Data Protection Policy
- Records Management Policy
- Freedom of Information Procedure
- Information Governance Policy and Framework
- Information Handling Policy
- Risk Management Policy
- Incident Reporting Policy

And their associated procedures (including but not limited to)

- Individual Rights and SAR Procedure
- Privacy Impact Assessment Policy and Procedure
- Anti-Fraud Policy
- Anti-Bribery Policy
- Freedom to Speak Up Policy
- Internet Social Media Policy

12. LEGAL REFERENCES AND GUIDANCE

- NHS Act 2006
- Data Protection Act 1998
- Human Rights Act 1998
- Computer Misuse Act 1990
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Health and Social Care Act 2012
- Crime and Disorder Act 1998
- The Children Act 1989 and 2004 Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)
- Public Interest Disclosure Act 1998
- Audit & Internal Control Act 1987
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Road Traffic Act 1988
- Regulations under Health and Safety at Work Act 1974
- Public Records Act 1958
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2012
- Coroners and Justice Act 2009
- Fraud Act 2006
- Bribery Act 2010
- Enterprise and Regulatory Reform Act 2013
- Equality Act 2010
- 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