Lincolnshire Community Health Services
NHS Trust

Information Security Policy

(Network Security, Computer Use, Email Procedure)

Reference No:	P_IG_27
Version:	2
Ratified by:	LCHS Trust Board
Date ratified:	
Name of author:	Data Protection Officer
Name of responsible committee:	Information Governance Management Assurance Group
Date approved by responsible committee:	21 April 2021
Date issued:	May 2021
Review date:	May 2023
Target audience:	All staff and third-party contractors employed by LCHS
Distributed via:	LCHS Website

Lincolnshire Community Health Services NHS Trust

Information Security Policy

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/Amended by
1		Amalgamation of policies P_IG_07, 09 13, 21 content previously ratified and further content updated to reflect GDPR.	June 2018	Kaz Scott
2		Full Review UK GDPR	Feb 2021	Kaz Lindfield-Scott
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Lincolnshire Community Health Services NHS Trust

Information Security Policy

Contents

i)	**Version Control Sheet**	**Page**
ii)	**Policy Statement**	
	Information Security	5 - 7
	Network Security	8 - 11
	Computer Use	12 - 19
	Email Procedure	20 – 23
	NHSR Monitoring	23
	Equality Impact Analysis	24

Lincolnshire Community Health Services NHS Trust

Information Security Policy

Policy Statement

Background	This policy is a requirement under ISO 27001:13 and sets out the security management system for the Trust.
Statement	This document is a key component of the overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures. • COIN/HSCN Policy • Incident Reporting Policy • Information Governance Management Policy
Responsibilities	The Head of Digital Health has been designated as responsible for Information Security.
Training	Training will be facilitated via the Trust induction and mandatory annual training.
Dissemination	The policy will be published on the Trust website.
Equality Statement	As part of our on-going commitment to promoting equality, valuing diversity and protecting human rights, Lincolnshire Community Health Services NHS Trust is committed to eliminating discrimination against any individual (individual means employees, patients, services users and carers) on the grounds of gender, gender reassignment, disability, age, race, ethnicity, sexual orientation, socio-economic status, language, religion or beliefs, marriage or civil partnerships, pregnancy and maternity, appearance, nationality or culture

INFORMATION SECURITY

Information Security (IS) is a key component of the Trust's overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

Information is collected and recorded in a number of mediums including paper and digital. The Trust has well developed infrastructures and arrangements to support information security. It shares some of these arrangements with other health providers (NHS and Non-NHS) to develop shared care and information sharing agreements. Where a contractual arrangement is linked to the provision of services, there is a clear expectation partner organisation will maintain the same levels and approaches to Information security.

Accountability for IS resides, ultimately, with The Chief Executive, senior partners or equivalent responsible officers. This responsibility is discharged through a designated member of staff, the Head of Digital Health who has lead responsibility for managing and implementing related procedures within the Trust.

Objectives

The objectives are to preserve:

- **Confidentiality** - Access to data shall be confined to those with appropriate authority and legitimate rights and relationships
- **Integrity** – Information shall be complete, accurate and up-to-date. All systems, assets and networks shall operate correctly, according to specification
- **Availability** - Information shall be available and delivered to the right person, at the time and place when it is needed

Aim

To establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust by:

- Ensuring staff are aware of and fully comply with the relevant legislation
- Describing the principles of security and explaining how they will be implemented
- Introducing a consistent approach to security, ensuring staff fully understand their responsibilities
- Creating and maintaining a level of awareness of the need as an integral part of the day to day business
- Protecting information assets under the control of the Trust

Scope

This applies to all information, information systems, networks, applications, locations and users of the Trust or supplied under contract to it.

Responsibilities

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

- Its application in their work areas, personal responsibilities and how to access advice on information security matters

All staff shall comply with 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 the physical environments where information is processed or stored.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and ensure the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

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

Legislation
The Trust is obliged 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 the Trust, who may be held personally accountable for any breaches.

The Trust shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act 2018, UK General Data Protection Regulation
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Health and Safety at Work Act 1974
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- The Privacy and Electronic Communications Regulations (PECR)
- Freedom of Information Act 2000
- Health & Social Care Act 2012

Awareness Training

- This will be included in the staff induction process and align with the IG/DP Training to ensure that staff awareness is refreshed and updated as necessary

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause
- Expectations of staff shall be included within appropriate job definitions

Security Control of Information Assets
Each information asset shall have a named Information Asset Owner (IAO) who shall be responsible for that asset.

Access Controls
Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

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

Computer Access Control
Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

Application Access Control
Access to data, system utilities and program source libraries will 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 the availability of a licence from the supplier.

Equipment Security
Any assets, equipment shall be physically protected from threats and environmental hazards. Where possible this will include protecting equipment through strong password protection and encryption in line with national guidelines.

Information Risk Assessment
Once identified, risks shall be managed on a formal basis. They will be recorded within a risk register and action plans put in place to effectively manage those risks. The risk register and all associated actions will be reviewed at regular intervals. These reviews help identify areas of continuing best practice and possible weakness and potential risks that may have arisen since the last review.

Events and weaknesses
All events and suspected weaknesses are to be reported in accordance with the Incident Reporting Policy. All information security events shall be investigated to establish their cause and impacts.

Protection from Malicious Software
The Trust shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff are expected to co-operate fully and will not install software on the Trusts' equipment without authorisation.

User media
Removable media of all types that contain software or data from external sources, or that have been used on external equipment, must also be fully virus checked before being used on Trust equipment. Port Control is in place to prohibit the use of any unapproved devices.

Monitoring System Access and Use
An audit trail of system access and data used by staff shall be maintained and reviewed on a regular basis.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects there has been a breach of policy for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime or in the interests of national security
- Ascertaining or demonstrating standards using the (quality control and training)
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system
- Any monitoring will be undertaken in accordance with the Human Rights Act

Accreditation of Information Systems
The Trust shall ensure all new information systems, applications and networks include a security plan and are approved before they commence operation.

System Change Control
Changes to information systems, applications or networks shall be reviewed and approved through the system process.

Intellectual Property Rights
The Trust shall ensure all information products are properly licensed and approved. Users shall not install software on the Trust equipment and any breach may be subject to disciplinary action.

NETWORK SECURITY

The network is a collection of communication equipment such as servers, switches, routers, hubs, computers, and printers, which have been connected together by cables or means of other wireless technologies. The network is created to share data, software, and peripherals such as printers, Internet connections and data storage equipment.

Network Security applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

This document also sets out the protection of the confidentiality, integrity and availability of the network, establishes the security responsibilities for network security.

Aim

The aim of this policy is to ensure the security of the Trust network.

- Ensure Availability
- Ensure the network is available and secure for users
- Preserve Integrity
- Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets
- Preserve Confidentiality
- Protect assets against unauthorised disclosure

Scope

This applies to all networks within the Trust used for:

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images

Principles

The network will be available when needed, will be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, the Trust will undertake the following;

- Protect all hardware, software and information assets under its control by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that commensurate with the risks to its network assets.
- Implement in a consistent, timely and cost effective manner.

Risk Assessment

The Trust will where appropriate, carry out security risk assessment(s) in relation to all the business processes. These risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Risk assessment will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the network. Formal risk assessments will conform to ISO27001:13.

Physical & Environmental Security
Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

The Network Security process will ensure only authorised staff hold door entry fobs and the list of authorised users is reviewed periodically. Any breach should follow the Incident Reporting process.

Critical or sensitive network equipment will be protected from power supply failures.
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 Trust staff and 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 Trust will ensure all relevant staff are made aware of procedures for visitors and escorted when necessary.

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.
- There must be a formal, documented user registration and de-registration procedure for access to the network.
- Departmental managers must approve user access.
- Access rights to the network will be allocated on the requirements of the job role
- Security privileges (i.e. 'local 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 appropriate documentation is complete
- All users will have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret (see User Responsibilities).
- User access rights will be immediately removed or reviewed for those users who have left the Trust or changed jobs.
- Third party access to the network is based on a formal contract that satisfies all necessary NHS security conditions. All third party access to the network must be logged.

External Network Connections
The ICT processes will ensure;

- Any connection to external networks and systems have documented and approved
- Any connection to external networks and systems conform to the NHS-wide Network Security Policy, Statement of Compliance and supporting guidance.
- Approve all connections to external networks and systems before they commence operation.

Maintenance Contracts
Maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Trust's Asset register.

Data and Software Exchange
Formal agreements for the exchange of data and software between organisations must be established and approved by the Trust.

Fault Logging
The Trust will ensure that a log of all faults on the network is maintained and reviewed under the ICT process.

Network Operating Procedures
Documented operating procedures should be prepared for the operation of the network, to ensure its correct, secure operation.

Data Backup and Restoration
Ensuring that backup copies of network configuration data are taken regularly and storage of backup tapes. All backup tapes will be stored securely, and a copy will be stored off-site and retained for the appropriate amount of time for statutory and legal purposes, including the safe and secure disposal of backup media.

User Responsibilities, Awareness & Training
All users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

Accreditation of Network Systems
Accreditation ensures the network is approved before it commences operation. ICT are responsible for ensuring the network does not pose an unacceptable security risk to the Trust.

Security Audits
This will require checks on, or an audit of, actual implementations based on approved security policies.

Malicious Software
Ensure measures are in place to detect and protect the network from viruses and other malicious software.

Secure Disposal or Re-use of Equipment
Where equipment is being disposed of, the ICT process must ensure all data on the equipment (e.g. hard disks or tapes) is securely overwritten. Where this is not possible staff should physically destroy or dispose of through an Approved Trust Contractor.

Monitoring
Ensure the network is monitored for potential security breaches and comply with current legislation.

Reporting Security Incidents & Weaknesses
All potential security breaches must be investigated and reported. Security incidents and weaknesses must be reported in accordance with the requirements of the incident reporting procedure.

System Configuration Management
Ensure that there is an effective configuration management system for the network.

Business Continuity & Disaster Recovery Plans
The Trust must ensure that business continuity and disaster recovery plans are in place.

Unattended Equipment and Clear Screen

Users must ensure they protect the network from unauthorised access and log off the network when finished working.

The Trust operates a clear screen process that means users must ensure any equipment logged on to the network is protected if they leave it unattended, even for a short time. Workstations must be locked, or a screensaver password activated. Users failing to comply may be subject to disciplinary action.

Apps
Only approved apps are to be used on Trust issued equipment and any involving PII must go through the Data Protection Impact Assessment process.

ICT Process
- To produce and implement effective security countermeasures.
- Produce all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of the Network Security.

Data Protection Security Process
- Implementing an effective framework for the management of security and assisting in the formulation of programme and related policies.
- Produce standards, procedures and guidance on and co-ordinate activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on matters, including representation on cross-community committees.
- Advising users of information systems, applications and networks of their responsibilities.
- Advising the SIRO and Caldicott Guardian on risks and security matters and recommending actions.
- Encouraging, monitoring and checking compliance, promoting awareness and providing guidance and advice.
- Incidents or alerts have been reported that may affect systems, applications or networks.
- Providing advice and guidance on:

    - Policy Compliance
    - Incident Investigation
    - IT Security Awareness
    - IT Systems Accreditation
    - Security of External Service Provision
    - Contingency Planning for IT systems

Line Manager's Responsibilities
Ensuring the security of the network, that is information, hardware and software used by staff is consistent with legal and management requirements and obligations. To ensure staff are made aware of their security responsibilities and have had suitable training.

General Responsibilities
All personnel or agents acting for the Trust have a duty to:
- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the Trust's IT systems.
- Report on any suspected or actual breaches in security.

COMPUTER USE
This covers the following areas for acceptable use:

- Responsibilities and use of IT assets
- Use of e-mail and Internet
- Use of mobile devices, removable media and remote access
- Network usage (Including passwords/user access control)
- User declaration

All staff will be required to read and sign this document and be appropriately authorised by their manager prior to gaining access to the IT network.

Scope
This applies and includes all community health services managed by the Trust. It describes the responsibilities and acceptable use of IT and Information assets within the Trust.

This applies to all those working for the Trust, in whatever capacity. A failure to follow the requirements may result in investigation and management action being taken as considered appropriate.

This may include formal action in line with disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to civil or criminal action being taken.

Definitions
Where referenced the term 'data' may refer to either the business data or Personally Identifiable Information (PII) – either staff or patient.

Offensive material includes but is not restricted to: hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disabilities.

Trust's Computer System, comprises:

- All network infrastructure including cables, wired and wireless access points.
- Cloud Technology and Data Storage e.g. OneDrive and SharePoint
- Network hardware including servers, storage and communications equipment.
- Personal hardware, i.e. desktop PC's & laptops.
- Printers and Multi-function devices (MFD)
- Peripheral equipment such as, keyboards, mice and drawing tablets
- All major software applications and generally installed software, plus any additional software installed on the Trust computer system.
- Portable device; Smartphone's, tablets, cameras and any other external device when connected either directly or wirelessly and only Trust issued equipment is supported.

All removable media i.e. CDs/DVDs, memory sticks/flash drives, external hard disk drives and any other data storage device.

Information Asset
Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation.

Confidentiality
Ensuring personal, sensitive and/or business critical information is appropriately protected from unauthorised access and only accessed by those with a legitimate business need.

Personally Identifiable Information (PII)
Is any data that could potentially be used to identify a particular person. **Examples** include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.

Corporate Sensitive Data
Information about the business functions of the Trust, which could be commercially valuable, such as financial or contracting information.

Spam
Mass unsolicited electronic mail received from an un-requested source which attempts to convince the user to purchase goods or services. SPAM consumes valuable network resources while delivering no business benefit.

Blogging and Social Networking Sites
The use of blogging and social networking websites can expose the Trust to information risks, even where these sites are not accessed directly from work. The popularity of such websites and the rapid growth of internet enabled devices such Smartphones and tablets has resulted in significant awareness and uptake of these websites from home, work and when mobile.

The risks that this may pose include:

- Unauthorised disclosure of business information and potential confidentiality breach.
- Legal liabilities from defamatory postings etc. by staff
- Reputational damage to the Trust
- Staff Intimidation or harassment with possibility of personal threat or attack against the blogger, sometimes without apparent reason.
- Identity theft of personal data that may be posted
- Malicious code and viruses causing damage to IT infrastructure
- Systems overload from heavy use of sites with implications of degraded services and non-productive activities, particularly in the use of rich media (such as video and audio) becoming the norm.

Phishing
This is the attempt to obtain sensitive information such as usernames, passwords, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication i.e. Emails, SMS, instant messaging.

Responsibilities for Acceptable Use of ICT Assets
Staff may only use assets, which are specifically authorised by their line manager, in accordance with this policy.

Unauthorised use, modification, removal of information assets is strictly prohibited. Where assets are needed to be removed off-site, management approval for the removal of such assets must be obtained.

Acceptable use of Email and Internet
Staff can use its e-mail and internet professionally, ethically and lawfully without compromising the security of the Network and whilst maintaining confidentiality. However, their use can expose the Trust to technical, commercial and legal risks if they are not used sensibly.

Permitted and Prohibited Uses
Staff should only access the Internet if such use is required as part of your job, primarily for healthcare related purposes. Limited and reasonable personal use is permitted as long as it does not interfere with the performance of duties.

The Internet must not be used for gambling, illegal activity, including personal business use.

The Trust's may use automated content filtering software to restrict access to categories of websites that are deemed to be inappropriate, e.g. Adult/sexual, violence, criminal, etc. These are subject to on-going review. However if staff are able to access a particular website it may not always mean that it is permitted.

Inappropriate or excessive personal use may result in disciplinary action and/or removal of e-mail facilities. Staff should be aware that both private and legitimate business use of e-mail will be subject to monitoring. There is no absolute right for staff to use the e-mail facilities for personal use and should be limited to Trust business activities only.

Offensive, Illegal and Defamatory Materials
Staff must not under any circumstances use the e-mail system or internet facilities to access, download, send, receive or view any materials that will cause offence to any person by reason of;

- Any sexually explicit content;
- Any sexist or racist remarks;
- Remarks relating to a person's sexual orientation, gender reassignment, race, ethnicity, political convictions, religion, disability or age.

Staff must not under any circumstances use the e-mail system or Internet to access, download, send, receive or view any materials that you have reason to suspect are illegal.

Copyright
E-mail and internet users must observe all contractual, copyright issues. Under the Copyright, Designs and Patents Act 1988, copyright law can be infringed by making an electronic copy or making a 'transient' copy (which occurs when sending an e-mail).

Copyright infringement is becoming more commonplace as people forward text, graphics, audio and video clips by e-mail. Employees must not copy; forward or otherwise disseminate third-party work without the appropriate consent.

Malware, viruses and spam
Non-text e-mail attachments (e.g. software, computer games, executable files, bitmaps) and software downloaded from the Internet may contain computer viruses or other harmful content which can seriously disrupt the Trust's computer systems and network.

Any employee who knowingly distributes a computer virus or any harmful code or spam using the Trust's e-mail system or network will be subject to disciplinary action which may lead to dismissal.

Housekeeping and Good Practice
The following rules will help systems to work more efficiently.

- Messages should be reviewed and deleted on a regular basis and, if necessary, archived in accordance with the NHS Records Management: Code of Practice 2020.
- Where possible, obtain confirmation from the recipient that an important e-mail has been received.

Corporate Access
In the case of unexpected leave, e.g. long-term sick, managers should attempt to obtain consent from the individual to access their email and/or network drive. If this is not possible managers should seek advice from their Senior Manager regarding access to the individuals account.

Each case will be assessed individually based on the impact and disruption it may have to the local services.

Legal Issues relating to use of email and the Internet
This section is intended to provide staff with guidance on the most important legal issues which may arise from their use of the e-mail system and Internet access.

It is very important this section is read and to understand those issues as this will help staff, and the Trust, to avoid problems.

These are not just theoretical issues. If the law is broken then this could lead to one or more of the following consequences:

- Civil and/or criminal liability for yourself and the Trust disciplinary action against staff including your dismissal. Ignorance of the law is not a defence in court.

Bullying and Harassment
The Trust requires all employees to be treated with dignity at work, free from harassment and bullying of any kind. It is strictly forbidden to send messages that contain offensive or harassing statements or language, particularly in respect of race, national origin, sex, sexual orientation, age, disability; religious or political beliefs. Remarks sent by e-mail that are capable of amounting to harassment may lead to complaints of discrimination under the Equality Act 2010. Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal.

If subjected to or know about any harassment or bullying, whether it comes from inside or outside the Trust, staff are encouraged to contact their line manager / HR Advisor immediately.

Formation of Contracts
E-mail is capable of forming or varying a contract in just the same way as a written letter. Such capability gives rise to the danger of employees inadvertently forming contracts on behalf of the Trust or varying contractual terms to which the Trust then becomes bound.

Defamation by E-mail or Internet
The ease of use of e-mail can lead to unguarded and impetuous comments being made, which in turn could be classified as defamatory. Defamation arises where there is the publication of an untrue statement tending to lower the subject of the statement (which may be an individual or an organisation) in the estimation of the public generally. Liability for the tort of defamation applies to electronic communication as well as traditional publishing.

Any expression of fact, intention and opinion via e-mail can be held against the author and/or the Trust, therefore do not include anything in an e-mail you are not prepared to account for or defend. Employees are therefore advised to take care when drafting e-mails to ensure they do not send messages that might be defamatory, incur liability on the part of the Trust or adversely impact on the image of the organisation.

Obscene Materials
Staff must not under any circumstances use the e-mail system or Internet to access, display, circulate or transmit any material with a sexual content. This may constitute a criminal offence and both the Trust, and the employee may be personally liable. Sexual harassment will be treated as a serious disciplinary matter which may lead to dismissal.

Protection of Personal Data
The Trust is required to comply with the DPA concerning the protection of personal data. Failure to adhere to legislation could expose the Trust to civil liability and enforcement action by the Information Commissioner Office (ICO)

Obligations under legislation are complex and staff can ensure compliance by adhering to the following rules:

- Do not disclose any information about a person in an e-mail or on the Internet which you would object to being disclosed about yourself.
- Be particularly careful when dealing with sensitive information concerning a person's racial or ethnic origin, sexual life, political beliefs, trade union membership, religious beliefs, physical or mental health, financial matters and criminal offences.
- Do not send PII using email unless the e-mail meets the required security standard e.g. (NHS.net).
- Do not send any personal data outside the European Economic Area.

Trust Computer Systems
The provision of the Trust's computer system is managed and maintained centrally by Information Communications & Technology Services (ICT).

In order to prevent damage, compromise or loss of Trust data, the following restrictions will apply to the use of mobile devices and removable media within the Trust:

- Only Trust owned / managed devices will connect to, or synchronise with, the ICT Systems. No privately owned devices can be used.
- The device should only be used for work related purposes
- PII must only be stored on encrypted devices.
- Encrypted USB devices must only be used for temporary data transfer and not long-term storage Data must not be transferred and stored on any personal equipment e.g. home PC.
- If media / data are no longer required by the user or the Trust, it should be securely erased or disposed by ICT.
- All removable media and mobile devices should be stored in a safe, secure environment in line with the policies and manufacturers recommendations.
- Smartphones must have a minimum of 8 digits password/passphrase applied.

In order to prevent damage, compromise or loss of Trust data, the following restrictions will apply to the use of mobile devices and removable media within the Trust:

- The Trust uses technical measures to enforce restrictions on the use of portable devices and removable media on USB ports and other connecting interfaces.
- Data stored on removable media should be backed up or transferred to the network at regular intervals. Appropriate security measures should be in place to protect the data on any back up media, including encryption of any PII and secure physical storage.
- All removable media and mobile devices must be returned to ICT services if the staff member leaves employment or no longer requires it for their job.

- Remote access to the Trust managed networks must be authorised by a Manager of the relevant service. Only Trust-owned laptops can be used for remote access and must be configured with necessary remote access and security software.
- Remote access users must ensure the security of their private broadband connection before using the remote access service. Extra security measures must be taken when using wireless broadband access by ensuring that encryption is enabled (password protected) on the wireless router as per manufacturer's recommendations.
- Remote access users to 'open zones' e.g. wireless access at cafes, to gain access to the Trusts network are not deemed secure and can result in unauthorised access.

Confidential Electronic Data in Transit
All PII held in portable electronic format **MUST be encrypted** in transit.

To enable continuation of care and service in the event of data loss in transit all data must be backed up to a network folder or another external secure device before it is removed from the security of an NHS site.

For physical transportation:
- A Trust laptop encrypted with Windows Encryption
- Trust issued encrypted USB memory sticks or external encrypted hard disk drives to AES 256 standard

For e-mail transportation:
- NHSMail – only between *nhs.net accounts or to other approved secure domains
- Encryption within an approved secure e-mail domain
- NHS Secure File Transfer (SFT) – requires a registered account

Responsibilities
Managers have overall responsibility for the security, safe custody and timely maintenance of all Trust computer equipment within their department.

Each member of staff is specifically responsible for:
- The security, safe custody and timely maintenance of all Trust computer equipment assigned to them and for reporting any security issues or concerns promptly to their manager.
- Ensuring equipment is not modified in any way unless through an ICT services formal change request.
- Maintaining computer equipment appropriately and reporting any faults via the Self-Service Portal and notifying their manager.
- To preserve the security of Trust's information asset:
- ONLY equipment owned by the Trust or ICT approved equipment belonging to partner organisations, including formally contracted or leased hardware, software, media and related equipment may be used:

Passwords/Passphrase
Everyone granted authorised access to the Trust's computer system is issued a password, which forms part of access credentials. Additional access credentials may be issued for corporate or clinical systems.

All password holders are responsible for:
- Changing a password/passphrase on first log on, when nearing expiry or if it has been compromised.
- Always keeping passwords private and confidential
- Never sharing passwords/passphrase with anyone, this includes managers.

- Never write down or record passwords where it can be accessed by someone else. Recording passwords securely can be in an Excel spreadsheet on the users Home Drive.
- Changing passwords on a regular basis.

Group or Shared passwords/passphrase
Only to be used by exception. It is accepted that sharing passwords/passphrase may be required in certain circumstances to facilitate team working, for example, sharing departmental office applications and equipment, such as:

- Access Databases, Excel Spreadsheets, Word documents, external encrypted devices, Training Room PC's & laptops or generically named operational NHS.net account.
- where access to a shared resource cannot be achieved in any other way.
- where all participants have physical access to the encrypted device or direct access to the folder containing the controlled shared document.
- All workstations should be secured when unattended i.e. by the use of screen lock or by logging off.

Password/Passcode Composition
The requirements and a complex one become much stronger and effective when:

- Between 8 – 16 characters long, contains different characters and uses upper, lower , numeric or special characters

Multifunction Devices (Printer/Scanner/Photocopier)
Multifunction devices copy, scan documents and images into the user's storage area and uses Smartcard technology to support these functions.

Security measures are in place to protect such data from unauthorised access with the technology to erasure and incorporated into these devices by the manufacturer.

Responsibilities of the Trust
The Trust must provide a 'Duty of Care' to all its employees by ensuring that, whilst within the workplace, they are protected from information and activities that are classed as 'socially unacceptable' or pose a threat to the Confidentiality, Integrity and Availability of the data.

Responsibilities of all Staff
It is the responsibility of the individual to ensure they understand their responsibilities. Managers are responsible for ensuring that staff have read and understand their obligations in relation to this Policy.

General and Targeted Monitoring
This may be undertaken to check efficiency, capacity and appropriate use. Monitoring of individual users will not be undertaken without their consent, unless routine monitoring (that does not identify an individual user), indicates unacceptable activity is taking place. This will only take place by exception and in response to:

- ICT request to resolve a technical issue or formal request for an investigation

The Trust has in place routines to regularly audit compliance with this and other policies and reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating / detecting unauthorised use, preventing or detecting crime or in the interests of national security
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system

Data Protection and Monitoring at Work
A number of the requirements of the DPA will come into play whenever an employer wishes to monitor workers. The Telecommunications Regulations 2000 provide that an employer retains the right to carry out monitoring despite the fact the employee has not given their express consent.

Automated monitoring may take place using audit and security software and intended to ensure that this is adhered to and that the Trust and its employees are acting lawfully.

Monitoring without consent will only be carried out with the authority of two Executive Directors / and or equivalent.

EMAIL PROCEDURE
E-mail is now established as a major communication tool and the Trust wishes to encourage the correct and proper use of e-mail, and expects staff to use this facility professionally, ethically and lawfully ethically without compromising the security of the Trust Network and whilst maintaining confidentiality.

The use of e-mail is intended primarily for Trust business related purposes or professional development and training that supports the goals and objectives of the Trust. Staff should therefore use e-mail primarily for the legitimate business of the Trust and within the bounds of their authority.

Scope
This applies to all directly and indirectly contracted staff and other persons working for the Trust or organisations hosted by us.

- All Trust employees whilst engaged in work for the Trust at any location, on any computer or internet connection
- Any other use by Trust employees which identifies the person as a Trust employee or which could bring the Trust into disrepute on any computer or internet connection
- Other persons working for/ with the Trust, persons engaged on Trust business or persons using Trust equipment and networks
- Anyone granted access to use Trust e-mail facilities or over the Trust network

Definitions
Where referenced within the term 'data' may refer to either the Trust's business data or PII – staff or patient.

Offensive material includes but is not restricted to: hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disabilities.

Responsibilities of the Trust
The Trust must provide a 'Duty of Care' to all its employees by ensuring that, whilst within the workplace, they are protected from information and activities that are classed as 'socially unacceptable' or pose a threat to the Confidentiality, Integrity and Availability of Trust data.

Responsibilities of all Staff
It is the responsibility of the individual to ensure they understand this policy. Managers at all levels are responsible for ensuring that staff have read and understand their obligations in relation to this.

Access and Authorisation
E-mail is available to all staff that are registered as users of the Computer Network. Staff may only use the e-mail service while they remain employees of the Trust.

Account Authorisation
Requests to authorise staff to receive e-mail services or to change an existing account holder's details must be submitted by an appropriate manager or they will not be approved.

Personal Use
Although personal use of e-mail facilities is discouraged, limited personal use is permitted provided it is consistent with the Trust's code of conduct and does not interfere with the performance of duties.

Employees should regard this facility as a privilege that should be exercised in their own time without detriment to the job. Inappropriate or excessive personal use may result in disciplinary

action and/or removal of e-mail facilities. Staff should be aware that both private and legitimate business use of e-mail will be subject to monitoring. There is no absolute right for staff to use the e-mail facilities for personal use.

Confidentiality
To avoid compromising confidentiality e-mail users should:

- work on the basis that e-mail is not entirely immune to interception
- ensure consent has been given before releasing PII to third parties
- Never send PII using a personal e-mail over the Internet (e.g. Hotmail, Gmail etc.)

When responding by e-mail, staff should be aware that the e-mail account may belong to a family group or a member of the family other than the data subject (i.e. the patient). Unless the data subject has given their express consent, communication by this means may result in a breach of confidentiality and should be avoided.

Viruses
Viruses can damage computer systems, destroy data, cause disruption and incur considerable expense for the Trust. Employees must not open attachments from external sources unless they are sure of their authenticity. If in doubt seek clarification from the sender.

If any viruses are found or you suspect a machine may be infected, disconnect the equipment from the network, including switching off wireless connectivity and inform the ICT Service Desk **immediately.**

It is forbidden to send executable computer programme files as attachments due to the risks they pose. The downloading and subsequent use of any software received via e-mail, without the prior approval of the Trust, is strictly forbidden (this includes screen savers).

It will be considered a serious breach if an e-mail user deliberately infects or makes any attempt to infect the Trust or other network system with computer viruses.

Sending and receiving e-mail messages

- Use e-mail only when it is the most appropriate means of communication
- Communicate only with those who are required to read the message
- Use the Global Address Book with care to ensure e-mail reaches the correct recipient

Large number of recipients
Be selective about who to send messages to and use BCC rather than a visible e-mail list.

Global e-mails
Global e-mails are only intended for communicating information relating to Trust business. Should you wish to reply to a global e-mail message ***only*** reply to the named contact at the bottom of the e-mail, Do not respond globally as this uses unnecessary storage space on the e-mail server.

Auto forwarding of e-mail
To avoid PII or sensitive information being sent on to an insecure e-mail address auto forwarding of e-mail from a Trust e-mail address to a personal e-mail address is not allowed.

E-mail received in error
Inform the sender if you receive a message sent to you in error. Delete the message from your mailbox. If an e-mail received in error contains PII, inform the recipient and complete an IR1.

E-mail with warnings about criminal activity / frauds/ scams

Where there are genuine matters relating to security that staff need to be aware of these will be notified by the Police to NHS Security Management specialists who in turn will issue warnings or guidance to staff. If you receive e-mail purporting to give warnings about criminal activity or scams please do not forward these on to colleagues.

Out of Office
Use the 'Out of Office' tool when appropriate. Staff should ensure the Out of Office message includes details of when they will be back in the office, who should be contacted in their absence and include contact e-mail addresses or telephone numbers.

General rules
E-mail users must not:

- Use other people's mail accounts to send e-mails
- Give others authority to view or amend a mailbox unless fully justified
- Engage in any activity, which is illegal, offensive or likely to have negative repercussions for the Trust
- Allow third parties to read PII in e-mails by leaving your screen in view
- Read other people's e-mails sent to someone else, without their express permission
- Create or send any offensive, obscene or indecent images, data or other material
- Initiate or propagate any provocative exchanges of e-mail, chain letters or junk e-mail
- Engage in unauthorised selling or advertising of goods and services
- Create or send messages that may constitute racial, sexual harassment or harassment on the grounds of a disability
- Send any unsolicited commercial or advertising material either to another user or organisation(s)
- Forge, use a false identity or anonymously send e-mails

E-mail disclaimer
Disclaimer text will automatically be added to any external e-mails that are sent. Staff should not add disclaimer text within their own signature panel. The addition of this text is designed to limit the Trust's potential liability with respect to information being communicated. The use of a disclaimer does not provide an absolute defence against breaches of confidentiality nor should it preclude the user from undertaking fundamental checks before sending the e-mail.

Signature panels
E-mail signatures should follow the Corporate format. Further details can be obtained from the Communications Team.

Monitoring of E-mail
The Trust has the ability and legal right to monitor e-mail usage. By using e-mail the employee consents to any monitoring the Trust considers to be appropriate. E-mail monitoring will be conducted in the most effective way to ensure compliance and in accordance with any current legislation. The Trust will always consider if any monitoring intrudes unnecessarily on an employee's privacy.

When monitoring takes place staff will be made aware of the purpose and extent of the monitoring to be carried out except for the purposes defined under "Monitoring without consent".

Staff have a right of access to information held on them, including information obtained through monitoring; such information may be withheld if by doing so would prejudice the detection of a crime.

Employees will be allowed to make representations about the information gathered through

monitoring where it may have an adverse impact on them.

NHSMail
May be used to send PII across the network and. external communications outside of the network should use an accredited or secure e-mail.

All e-mail addresses end in @nhs.net. If the contents are to remain secure in transit both the sender and recipient must use @nhs.net or an e-mail accredited as secure. A list of accredited secure e-mails is available on the NHSMail website.

Breach of Policy
Staff will be liable to disciplinary action if they are in breach of e-mail procedures and depending on the severity of the offence may be liable to summary dismissal.

The distribution of any information via e-mail is subject to UK law and any illegal use will be dealt with appropriately. E-mails both in hard copy and electronic form, are admissible in a court of law.

If staff conduct and/or actions are unlawful or illegal the individual may be personally liable.
In the event of an accidental breach, staff members must advise their line manager immediately so that appropriate steps can be taken to mitigate or remove any possible risk(s).

Rights of Access
E-mails may be required to support a request from a Data Subject and are releasable by law where an individual can be identified.

NHSR Monitoring

Minimum requirement to be monitored	**Process for monitoring e.g. audit**	**Responsible individuals/ group/ committee**	**Frequency of monitoring/audit**	**Responsible individuals/ group/ committee (multidisciplinary) for review of results**	**Responsible individuals/ group/ committee for development of action plan**	**Responsible individuals/ group/ committee for monitoring of action plan**
DSPT Standards	Review / Audit / Reports	DPO	Annual	DPO / IGMAG	DPO / IGMAG	DPO / IGMAG

Equality Impact Analysis Screening Form

Title of activity	Information Security Policy		
Date form completed	Mar 2021	Name of lead for this activity	Kaz Lindfield-Scott

Analysis undertaken by:		
Name(s)	Job role	Department
Kaz Lindfield-Scott	Data Protection Officer	Data Protection and Compliance

What is the aim or objective of this activity?	To provide effective management and accountability governance structures, processes, policies and procedures and a comprehensive IG/DP training adequately resourced to manage and embed IG and DP throughout the Trust.
Who will this activity impact on? *E.g. staff, patients, carers, visitors etc.*	All Staff and Service Users

Potential impacts on different equality groups:

Equality Group	Potential for **positive** impact	**Neutral** Impact	Potential for **negative** impact	Please provide details of how you believe there is a potential positive, negative or neutral impact (and what evidence you have gathered)
Age	☐	☒	☐	
Disability	☐	☒	☐	
Gender reassignment	☐	☒	☐	
Marriage & civil partnerships	☐	☒	☐	
Pregnancy & maternity	☐	☒	☐	
Race	☐	☒	☐	
Religion or belief	☐	☒	☐	
Sex	☐	☒	☐	
Sexual Orientation	☐	☒	☐	
Additional Impacts	☐	☒	☐	

If you have ticked one of the above equality groups please complete the following:

Level of impact

	Yes	No
Could this impact be considered direct or indirect discrimination?	☐	☒
If yes, how will you address this?		

	High	Medium	Low
What level do you consider the potential negative impact would be?	☐	☐	☐

If the negative impact is high, a full equality impact analysis will be required.

Action Plan

How could you minimise or remove any negative impacts identified, even if this is rated low?
How will you monitor this impact or planned actions?
Future review date: