University Hospitals of Derby and Burton
NHS Foundation Trust

TRUST POLICY FOR INFORMATION TECHNOLOGY AND CYBER SECURITY

Reference Number:	**Version:** 1.2		**Status:** Draft	**Author:** M Chester **Job Title:** Head of IT
Version / Amendment History	**Version**	**Date**	**Author**	**Reason**
	1	June 2019	M Chester	New combined policy for UHDB
	1.1	Nov 2019	M Chester	Addition of temporary user
	1.2	Sept 2021	M Chester	Revision to include Log retention policy and process plus N365

Intended Recipients: All Trust staff, visiting staff from other organisations, employees of temporary employment agencies, third party users and contractors.

Training and Dissemination: Training and awareness provided at Trust Induction, regularly arranged IT Training Sessions and regular publicity in Synapse. Dissemination via the Trust Intranet.

To be read in conjunction with: Disciplinary Policy - Trust Policy and Procedure, Information Governance - Trust Policy and Procedure, Trust Policy and Procedure for Incident Reporting, Analysing Investigating and Learning, Freedom to Speak Up (Raising Concerns at Work) - Trust Policy and Procedure, Mobile Devices / Mobile and Landline Telephony - Trust Policy and Procedure, Policy and Guidelines for Data Protection and Confidentiality (Dealing with Confidential Information) - Trust Policy and Procedure; Conflicts of Interest - Management of - Trust Policy and Procedure

In consultation with and Date: IT and Information Services; Staff Representatives; Information Governance Team.

EIRA stage one Completed

EIRA Stage two Completed N/A

Approving Body and Date Approved	Trust Delivery Group
Date of Issue	November 2021
Review Date and Frequency	November 2023 / 2 yearly
Contact for Review	Head of IT
Executive Lead Signature	Executive Medical Director

Contents

1. Introduction

University Hospitals of Derby and Burton NHS Foundation Trust (the Trust) is obliged to abide by all relevant UK legislation and other relevant legislation from the European Union. This requirement devolves responsibility to the employees and agents of the Trust, who may be prosecuted, if found to be in breach of any of the following acts. Three main laws apply – the Data Protection Act (2018), the Copyright, Designs and Patents Act (1988), and the Computer Misuse Act (1990). In addition, the Caldicott Report; which centres on the protection and use of Patient Information; has a particular bearing on the way in which information can or cannot be used. The main requirements of each of these Acts and of the Caldicott Report are outlined in this Policy. Employees are required to adhere to these as part of their contractual terms of employment.

Threats come from 2 main sources now. Firstly, the legitimate user who simply uses their access to do the wrong thing at the wrong time or who acquires a colleague's password in order to explore parts of a system to which they have not been given access. Networked systems are designed to make data available in many different places concurrently. Whilst this provides obvious benefits, the consequence of this is that the policing of the system becomes much more difficult because we are no longer dealing with just one machine in a single room.

Secondly, with the increased use and reliance on email and the day to day use of the internet; cyber threats such as Malware, Ransomware, Phishing attacks and Denial of Service (DoS) attacks (plus many others), are becoming more prevalent. These types of attack are highly sophisticated and frequently will trick the user into carrying out a common task, such as opening an attachment in an email to infect a PC and computer network. It is these types of attack that are now proving to be more of a challenge to defend against.

2. Purpose and Outcomes

Throughout the IT industry, it is widely acknowledged that it is not possible to provide 100% systems security. Therefore, the purpose of this Policy is to ensure that:

- All information systems within the Trust are properly assessed for all aspects of their security; this is recorded in the System Specific Security Policy (SSSP).
- Regular Disaster Recovery reviews are carried out on key systems
- The Confidentiality, Integrity and Availability of the Trust's Information Systems are preserved to the highest possible levels
- Systems are not susceptible to attacks that may lead to destruction, denial, accidental disclosure and unauthorised modification.
- All staff are aware of the limits of their authority and accountability.

The key is making sure that proper Information Technology and Cyber (IT&C) Security techniques are in use and in ensuring that users are fully aware of their responsibilities. To achieve a sound level of IT&C Security, it is necessary to train users about the likely consequences of not complying with Information Security Policies. This will be delivered via mandatory IG training delivered at staff induction sessions, e-learning and guidance documentation that is provided for staff.

This Policy aims to:

- Ensure that all members of Trust staff are aware of and comply with relevant legislation as described in this policy document.
- Describe the principles of IT&C Security, and how they will be implemented within the Trust
- Introduce a consistent approach to IT&C Security across all sites and locations and to ensure that all members of staff understand their own responsibilities
- Create and maintain within the Trust a level of awareness of the need for IT&C Security as an integral part of the Trust’s day to day business.

It will apply to:

- All automated information systems under the direct control of the Trust and those information services provided from National and other NHS Organisations
- All employees, temporary employees and agents of the Trust
- All employees and agents of other organisations who, directly or indirectly, make use of, or support the use of information systems under the direct control of the Trust. System Administrators will provide a copy of the Information Security Policy to members of these organisations.

3. Definitions Used

Information Technology Security Incident	A general definition of an Information Technology Security incident would be the misuse of Information Systems and the data held within these systems or the misuse of Trust IT equipment or services.
Cyber Security Incident	An incident that threatens the security, confidentiality, integrity or availability of the Trusts information assets, information systems or networks that deliver those systems and disrupts the normal business of the Trust
Investigation	An investigation is an inquiry into circumstances surrounding an actual or suspected incident. Examples of Information Technology and Cyber Security Incidents are included in Appendix 1.
Person Identifiable Data (PID)	Person Identifiable Data is information that can be used to identify a person e.g. name and private address, name and home telephone number etc.
Password	A password, PIN (Personal Identification Number), smartcard, security token or other means of securely restricting access to a system. It is for the sole use of the individual to whom it was assigned.
Sensitive Information	Information relating to a person’s: • racial or ethnic origin • political opinions • religious beliefs or beliefs of a similar nature • trade union membership

	• physical or mental health or condition • sexual life • offences or alleged offences and information relating to any proceedings for offences committed or allegedly committed by a person, including the outcome of those proceedings. **OR** relating to confidential business issues (i.e. Human Resources, Finance and contracts).

4. Key Responsibilities

Director of Digital Services / Chief Information Officer (CIO)	Overall responsibility for Information Technology and Cyber Security is to be assumed by the Chief Executive of the Trust. This responsibility is delegated to the CIO
Senior Information Risk Owner (SIRO)	The SIRO is responsible for ownership of information risk across the Trust. The SIRO acts as advocate for information risk on the Board and provides written advice to the accounting officer on the content of their Statement of Internal Control in regard to information risk.
Caldicott Guardian	The appointed Caldicott Guardian must approve all procedures that relate to the use of patient and service-user information and is responsible for enabling appropriate information sharing.
Head of Information Governance / Data Protection Officer (IG)	The Head of IG ensures that the Trust has a managed and coordinated standard based approach to Information Governance, providing staff with clear policies and procedures that ensure the organisation meets its statutory and legal obligations. The Head of IG is responsible for the completion of the annual assessment against the standards identified in the Data Security and Protection Toolkit and its subsequent submission to the Department of Health.
Deputy CIO – (Digital Programme and Systems)	The Deputy CIO – (Digital Programme and Systems) is responsible for ensuring the functioning of IT clinical systems in support of the identifying, recording, reporting to management, appropriately investigating and learning from incidents.
Head of Information Technology (IT)	The Head of IT is responsible for obtaining and providing advice on all Information Technology and Cyber Security matters. They also support the investigation and monitoring of access to the Trust IT systems to ensure and ensure they are being used acceptably. This includes audits of system access, malicious code attempts, Disaster Recovery testing, security policies and auditing of incident reports of Information technology and cyber

	security breaches.
Information Asset Owners (IAO)	The IAO is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. IAOs support the Trust SIRO in their overall information risk management function.
Information Asset Administrators (IAA)	The IAA is responsible for ensuring the Risk Assessment section of the System Specific Security Policy (SSSP) is completed and updated on an annual basis.
System Administrators	System Administrators will be responsible for the day to day operation of that part of the automated information system that they and / or their staff directly use, and for the information that they use and/or share with others. They are responsible in conjunction with the IAO for ensuring that an up to date SSSP is in place.
Line Managers	Line Managers are responsible for: • Informing the IT Service Desk when members of staff leave or move department in order for systems access to be amended appropriately • Highlighting any suspected breaches of this Policy to the IT Service Desk (See Appendix 1) • Requesting individual user logins from the relevant system administrators via the IT Service Desk • Ensuring that all staff receive appropriate training as part of their induction, and on an on-going basis as part of mandatory training, to enable them to carry out their work efficiently • Ensuring that everyone who uses an information system is competent to do so, appreciates the importance of providing correct information and fully understands the status of information produced (this will be done in conjunction with the user).
All Trust Staff	Individual users of any part of the Trust and NHS overall information architecture have specific responsibility to comply with the Information Technology and Cyber Security requirements which may be in force and remain individually accountable for actions carried out whilst using any computer system.
Information Governance Steering Group (IGSG)	The IGSG is chaired by either the Caldicott Guardian or the SIRO. It reports to the Trust Delivery Group (TDG). The group is attended by the SIRO and representatives from IT Services, Information Services, Records Management, Clinical Governance and Divisional Management Teams. Any information security issues will be highlighted here for relevant assessment and action.
IT & Cyber Security	The IT & Cyber Security Group is responsible for review

Group	all matters relating to IT and Cyber Security within the Trust. The Group is chaired by the Head of IT and report back to the Digital Services Senior Managers and the IGSG.
Digital Services Senior Managers Meeting	The Digital Services Senior Managers meeting is chaired by the Director of Digital Services. This group is responsible for monitoring all risks relating to IT, Cyber Security, Information and Information Governance.

5. Implementing the Policy for Information Technology and Cyber Security.

The Trust Board regard Information Technology and Cyber Security to be of vital importance.

Trust IT systems and equipment must only be used for work related tasks. Email is provided as a business tool, to improve communications throughout the Trust, both internally and externally. Internet connectivity is provided to facilitate a person’s work as an employee or student, specifically in terms of clinical, educational, training and research. Access is also encouraged to facilitate and improve health service management activities. Commercial work is unacceptable. All network activity and internet access is monitored by IT services. Employees must not access the internet for personal use during their working hours. Recreational use of Trust Internet access is limited to lunch breaks, work breaks and periods outside their working day.

Information Technology security risks are managed on a formal basis in accordance with the Policy for Incident Reporting, Analysing, Investigating and Learning. Incidents are recorded directly onto DATIX where necessary action plans are put into place to effectively manage the risks. Any implemented information Technology Security arrangements will be assessed and reviewed as part of the Trust risk management programme. This will identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the previous assessment / review.

5.1 Usernames and Password

All staff on joining the Trust will be issued with a username and password to access the Trust network together with any other usernames and passwords to access individual systems. These details are specific to the user and must not be shared with any other person. The user is responsible for all activity undertaken on their account, and could be disciplined for any inappropriate usage, whoever it is undertaken by. Furthermore, if a user is found to be sharing their security details (Passwords, Smartcard PIN or any other security detail issued to them) with another member of staff, disciplinary action will be taken against both members of staff.

Remember your account details are only for your use and **MUST NOT** be shared with anyone, including IT staff.

Staff are required to set a suitable password on their accounts which conforms to the following standards:

- The password must be a minimum of 8 characters
- It must contain at least 3 of the following 4 characters:
    - Uppercase letters
    - Lowercase letters

  - Numbers
  - Special characters (such as £$/?!><)
- Passwords must not contain sequences of characters such as 12345, qwerty, easy to guess words such as 'Password' or names.

Staff will normally be required to change their password every 90 days automatically, or immediately if there is a concern that an account may have been compromised or details shared.

5.2 Temporary User Accounts

When it is necessary to create a temporary user account for staff or visitors, then the account will be created as per a normal user account but an expiry date will be added to the network account so that the account expires at midnight on the day the user leaves the Trust. If that date is not known, then a maximum period of 3 months will be set on the account, and the line manager of the user will have to request an extension to the account if their period of employment goes beyond 3 months.

Once the account has expired, only the line manager can request for the account to be re-activated.

After 30 days the account and all associated user drives will be automatically deleted.

5.3 Administration User accounts

Normal user accounts allow users enough privileges to run all of the Trust systems. If a user requires an elevated level of access to allow them to support other users i.e. IT Services, then this higher level of access will be granted via a separate user account. This account will be easily identified as an Admin account by the addition of 'adm' to the username i.e. john.smithadm. As these accounts have elevated levels of access to the Trust network, certain restrictions will be in place on the account:-

- The account will not have any access to the Internet
- The account will not have any access to email
- The account must has a password of at least 16 characters rather than the normal 8, and include
  - At least 1 uppercase letter
  - At least 1 lower case letter
  - At least 1 number, and
  - At least 1 special character.

Admin accounts will only be issued to staff with the written permission of the CIO, Head of IT or Deputy Head of IT. All users with Admin accounts must sign an agreement as to how the account can be used and the consequences of misuse of the account. Any admin user found to be sharing their account or giving elevated privileges to their normal account may face disciplinary action.

5.4 Usage of the NHS mail system

NHS mail is based on the Microsoft 365 platform and by default gives staff access to email, Office online, Teams and SharePoint. The system is known within the NHS as N365.

All staff will be issued with access to the NHS mail system when joining the Trust. For staff joining from other organisations that use NHS mail, it may be possible for the user to re-use their existing account. In order for IT to reuse an existing account, the staff member must contact their previous Trust / employer and request that their account is marked as a leaver. Once this is done, the account can be transferred to the Trust.

N365 is a secure system and can be used for the storage and transfer of PID. For example, it can be used to email PID as long as it is being transmitted to another secure email system for example:

- nhs.net to nhs.net email is secure
- nhs.net to gov.uk email is secure
- nhs.net to outlook.com (Inc. hotmail.com) is not secure and should not be used for sending PID
- nhs.net to doctors.net is not secure and should not be used for sending PID

A full list of PID approved secure email systems can be found at:

https://digital.nhs.uk/services/nhsmail/the-secure-email-standard#list-of-accredited-organisations

If an email address is not found on this list, then it must be regarded as unsecure.

If there is any doubt about whether an email address is secure, the email can be sent via the NHS mail secure email service by adding [Secure] to the subject. Full details can be found in the Encryption Guide for NHS mail, which is on the NHS mail portal.

Your NHS mail account must not be used by any other person. You are responsible for all emails sent from your NHS mail account. If you believe that your account has been misused by another person, you must notify the IT Service Desk immediately.

NHS mail account passwords must be a minimum of 10 characters and follow the same standards as Trust passwords. However, it should be noted that you are only required to change your NHS mail password once every 365 days, unless your account has been compromised or you are forced to change your password by NHS mail.

The use of any other email system such as gmail, outlook.com, doctors.net etc. for Trust business is completely unacceptable. Anyone found using such systems for Trust business could be liable to disciplinary action.

5.5 Portable Data Storage Devices

The Trust now limits the use of portable data storage devices by the use of device blocking policies on all Trust machines as follows:

- Writing data to portable data storage devices is restricted to Trust issued memory sticks. These memory sticks can be obtained from IT Services. The memory stick is encrypted, and a secure password must be set up on the device before any data can be written to it. This ensures that if the stick is misplaced or stolen, any data written to it cannot be read. After 10 incorrect attempts to enter the password, the memory stick will be formatted and all data on the stick securely deleted.

- All other portable data storage devices are limited to read only access. This is to allow visitors to the Trust to access files and presentations held on their memory stick but it prevents them from writing any new data from a Trust machine.

In certain circumstances where there is a requirement to write data to a non-encrypted device, IT may allow this after a suitable risk assessment has been carried out.

5.6 Networked Systems

The Trust data network is a private network and access is only granted to authorised users to carry out specific functions. All traffic across the Trust Network is monitored using Intrusion Detection and prevention systems. Private equipment must not, under any circumstances, be connected to the network or any Trust IT equipment either via the wired ports, wireless or any other means. Accessing parts of the system(s) to which users have not been given access may result in disciplinary action.

All non-medical devices (laptops, PCs and tablets) connected to the Trust network must have operating system and software patches applied on a regular basis, to ensure that they are not susceptible to cyber-attacks. For medical equipment with either embedded or separate PCs attached, a full risk assessment will be carried out for each piece of equipment to determine the risk to the Trust network if the operating system cannot be patched. If necessary, the equipment will be isolated from the main Trust network to minimise the risk.

The IT Services Department and the Caldicott Guardian will conduct Information Technology and Cyber Security reviews at the request of System Administrators or because of a perceived need. The results of such reviews will be used to provide System Administrators with the appropriate guidance on the levels of security required for their systems.

Contracts with external organisations that use the information contained within Trust computer systems or provide support to systems must be in existence before such use can take place. These Confidentiality and Conduct Agreements for Third Party Service Provider contracts will dictate that all members of staff who work for the external organisation must comply with Trust Information Security policies, and that the external organisation is appropriately registered under the Data Protection Act (2018).

System Administrators will ensure that breaches of Information Technology and Cyber Security by external contractors are reported via the IT Service Desk to the IT Management Team in a timely manner, so that full investigations into the incident can be made. All security incidents will be reported on an IR1 in accordance with the Trust Policy for Incident Reporting, Analysing, Investigating and Learning.

Job descriptions for System Administrators include specific responsibility for the Information Technology and Cyber Security role. All Trust Information Systems must have at least two individuals with the appropriate level of expertise to administer the particular system. Any which are deemed critical as defined in the Disaster Recovery / Business Continuity Plan, must have at least three such individuals.

Any user accounts which have elevated levels of permission on the Trusts IT network must be separate from normal user accounts. These Admin accounts must be suitably identified and must not have access to email or the internet to prevent cyber threats gaining elevated security privileges. Any member of staff with such an Admin account will be required to sign an agreement outlining the appropriate use of that account.

The level of access to specific systems is determined on a Role Based Access basis, independent of organisational status. System Administrators are responsible for maintaining an accurate and up to date list of current users together with their access rights. In addition, System Administrators must ensure that levels of access are commensurate with the tasks that individual users will be required to perform and must carry out regular audits of the access control list.

5.7 Proactive Monitoring

In order for the Trust to protect its IT systems and data, a number of proactive cyber security monitoring tools are in place. These fall into 2 categories, front end systems that users see, and back end systems.

The main front end systems are:

- **Sophos Anti-Virus** – all PCs and laptops have Sophos anti-virus installed. This constantly monitors activity on the PC and is able to prevent or mitigate virus, malware, ransomware and other types of attack. Under no circumstances must staff attempt to disable this
- **Smoothwall Web Filtering** – all internet access in the Trust is monitored by Smoothwall. This prevents staff from accessing any site that is known to be dangerous and filters web traffic based on a number of pre-set criteria, such as gambling, pornography, violence etc. In some circumstances, a website may be blocked which staff need access to for work reasons. In those cases, a request can be made via the IT Service Desk to have a site unblocked. Smoothwall also keeps an audit log of all internet activity, and in cases of disciplinary action, the logs may be reviewed by HR.

The main back end systems are:

- **Darktrace Intrusion Protection System** – this is an intelligent system that monitors all network traffic across all Trust sites and looks for any activity that is ‘out of the ordinary’. If it detects such activity, then IT is alerted to this, and further investigations can be undertaken. This together with Sophos is the main line of defence against attacks such as WannaCry
- **Microsoft Advanced Threat Protection** – this is another monitoring system in place that also monitors activity on individual PCs and laptops and can alert IT to any unusual activity based on a predefined set of signatures. In addition to this information being available to the Trust, summary information is sent to NHS Digital so that they can get an overall picture on the levels of protection within the NHS.

In addition to the above systems, the Trust relies on other sources of information about Cyber-attacks. NHS Digital issue regular alerts and updates about Cyber Threats in the form of CareCERT alerts. These include a weekly bulletin of alerts as well as specific alerts directed at the Trust. As part of our Cyber Security process, these alerts are recorded as well as the actions taken for each alert. The National Cyber Security Centre also proactively issues information on new threats and cyber alerts, which the Trust reviews.

5.8 System Audit Log Retention

The Trust retains audit logs from all clinical systems plus logs from other key systems to enable key activity to be monitored. The logs are not proactively monitored, but the information is retained so that should there be any suspicious activity or cause to believe that a member of staff has accessed a system or patient information inappropriately, they can be reviewed to determine what activity has been carried out.

For systems that are on-premise, the logs are retained on the same servers as the system. For systems based offsite or in the cloud, the systems are either retained on the same servers as the system or on a separate log retention system.

For non-clinical systems including Active Directory, audit logs are retained for a period of 1 year.

For clinical systems, audit logs are retained for a minimum period of 1 year depending on the system

Requests for access to audit logs can only be made via a request from a General Manager with support from HR or an Executive Director. The request must be made in writing to the Director of Digital Services, Head of IT or the Head of EPR.

The full process for retention and access to audit logs can be found in Appendix 3.

5.9 Mobile Devices

The Trust is now making greater use of mobile devices for accessing patient data and systems. Where a mobile device is in use for such access, the device will be centrally managed and have a security policy in place which would enable the device to be wiped remotely or will wipe the device should some try to access it without the correct password. Any device that will be used to access Trust systems or data directly must be managed in this way.

Where staff wish to use their own device to access NHS mail, they should be aware that NHS mail will apply a security policy to the device. This policy will force the user to set up a passcode on the device (if one is not already present) and also encrypt the device. Users should be aware that if the incorrect passcode is entered on the device more than 8 times, the device will be factory reset and **ALL** data will be deleted. The Trust NHS mail and IT Services can take no responsibility for loss of any personal data, photographs etc. should this happen. It is the user’s responsibility to ensure that the data on their phone is regularly backed up if they choose to access NHS mail on a personal device.

Full details on setting up your mobile device to access NHS mail can be found on the NHS mail portal.

5.10 Cloud Computing and Hosting

As with many organisations, the Trust is starting to make increased usage of Cloud based services and external hosting of systems and websites in third party data centres. It is essential that steps are taken to ensure that the security of any such hosting arrangement meets the requirements of the Trust and that any data held in such cloud or 3rd party data centres are secure.

Any department looking at using such an arrangement must contact both IT and IG for approval before any contract can be placed. As part of the checks carried out, it may be necessary for the department to complete a Data Protection Impact Assessment (DPIA) to ensure that all GDPR requirements are met.

It will be necessary for IT to arrange for security testing of the Cloud Services or 3rd party hosting organisation before any system or website can go live. These checks will be carried out by an independent 3rd party Cyber Security organisation on the Trusts behalf. If any organisation refuses to allow such checks to be carried out, then the Trust will not contract for their services and an alternative must be found.

It will also be necessary for the checks to be repeated on a regular basis to ensure that the security of the Trust data remains to be up to necessary standards. The checks will be carried out on an annual basis or whenever there is concern about the security of Trust data.

Any contract with such 3rd parties must include an element of remediation within an agreed timescale should any security issues be found.

The use of any cloud storage such as iCloud, Dropbox, Google drive, One Drive (excluding NHS mail OneDrive for Business) etc. is expressly forbidden. Anyone found using such cloud storage for any Trust data may be liable to disciplinary action.

5.11 Data Backup and Recovery

All data held on the Trusts IT network is backed up daily, in line with the Trust Back-up process (see Appendix 2). This backup enables data and files to be recovered in the event of accidental deletion or corruption.

If users choose to store data or files local on a PC or laptop, IT Services cannot guarantee that it can be recovered should a device malfunction. For example, if a user chooses to save files to the desktop on a laptop, and the hard drive fails on the device, then those files will be lost and cannot be recovered. All users are provided with a personal network drive (U:\ Drive) which is where any personal files should be stored. Files which need to be accessed by other users should be saved to the departmental drive (S:\ Drive). These locations are secure and are backed up on a daily basis.

If data or a file becomes corrupt, then the user should contact the IT Service Desk and ask for the data to be recovered from the most recent backup.

5.12 Loan Equipment

The Trust makes use of a large amount of loan equipment, either as a trial of new technologies or as a replacement whilst equipment is repaired. It is essential that where loan equipment that has an attached laptop or PC is used within the patient environment, that PID is only entered into the device where absolutely necessary.

If any PID is entered onto the device, then the device must be passed on to IT to enable a forensic wipe of the PC or laptop to be carried out to ensure all patient data is completely removed. Any queries around this must be addressed to the Head of IT or Deputy.

5.13 General Information

It is the responsibility of the IGSG to ensure that procedures are in place to:

- Instruct all current and future staff in their Information Technology and Cyber Security responsibilities and ensure that they are provided with appropriate training for Trust systems before access is granted
- Ensure that unauthorised staff must not be allowed to access any system belonging to the Trust. Such access could compromise data integrity, and as such would be treated as a serious disciplinary offence

- Ensure that agency staff, locums, contractors and third-party users, who are not already covered by an existing contract which contains an appropriate confidentiality undertaking, sign a confidentiality agreement prior to being allowed access to Trust systems
- Ensure that all staff are aware of the Standing Orders on potential conflicts of interest
- Ensure that all staff sign appropriate non-disclosure undertakings as part of their contract of employment. However, staff need to be aware of the existence and requirements of the Public Interest Disclosure Act 1998 and Trust Freedom to Speak Up Policy
- Ensure that as part of their termination procedures, managers inform the IT Service Desk and/or appropriate System Administrators of the dates on which members of staff are due to leave the Trust, and the systems from which access rights need to be removed.

Users must continually strive to ensure that the confidentiality, integrity and availability of Trust information systems are preserved to the highest standards at all times. It is the responsibility of the individual user to ensure that passwords issued to them are not compromised and if they are, the individual is responsible for ensuring the password is changed.

All staff must have a signed contract of employment with the Trust, which must contain references to the need for maintaining a high standard of confidentiality. Unauthorised disclosure or misuse of PID / sensitive information may result in disciplinary action. It is the responsibility of each member of staff to be aware of the full nature of their responsibilities, which should be linked to key areas of each person’s job description.

5.14 Physical Security

It is the responsibility of every member of staff to ensure that they take all necessary steps to ensure that the Trust’s assets (Hardware, Information and software) are kept secure.

Staff must ensure when taking laptops, USB memory sticks or any device that contains Trust data, that they are stored securely and not left unattended at any time especially in public places. For example, staff must not leave laptops on the back seat or boot of their car. If a staff member takes a laptop home, they must ensure that the laptop is locked in the boot of the car, and then stored safely at home in a location to minimise the risk of theft (i.e. in a cupboard). If a laptop is stolen, then its theft must be immediately reported to the police, IT Services and Information Governance, so the risk of the loss can be determined.

Similarly, with USB memory sticks, staff must ensure that they keep any memory stick that contains PID, safely stored at all times either in a locked drawer or on their person. They should not be left unattended at any time, especially in public places. The loss of a memory stick containing PID must be immediately reported to both IT Services and Information Governance, so the risk of the loss can be determined.

When a work area is left unattended, even for short periods of time, all PID / sensitive information must be secured and where possible, the room locked. Areas that contain IT equipment must be locked when left unattended. This also applies to areas with controlled access. Where the area is open and cannot be locked (i.e. reception desks on corridors) the PC will be physically secured. When leaving PCs and laptops the device must be 'locked' so a password is needed to access it. PCs and laptops must be shut down and the monitors switched off when not in use.

No PID / sensitive information should be saved directly onto a PCs desktop. Any such material must be saved onto the secured network (i.e. a Personal Drive). Any PCs in high risk areas (where PCs are accessible and / or hold high levels of PID / sensitive information) or PCs with solid state hard drives plus all laptops and tablets are encrypted to a minimum of 256-bit encryption with strong password protection.

5.15 Disciplinary Processes

All Information Technology and Cyber Security breaches should be recorded on an incident report form (IR1), in accordance with the Policy for Incident Reporting, Analysing, Investigating and Learning. Line Managers must report all Information Technology and Cyber Security breaches to the Head of IG and Head of IT (Appendix 1). Where malpractice has been shown, appropriate disciplinary action must be taken, in accordance with the Trust Disciplinary Policy.

When suspected Information Technology Security breaches are reported, the Head of IG and Head of IT will investigate the suspected breach and report any serious Information Technology Security breaches to the Medical Director (Caldicott Guardian) who will then instigate a full either internal or external investigation as appropriate. Where investigations indicate or reveal mistreatment of children, this must be reported to the Trust Responsible Safeguarding Lead, Chief Executive and police. Full records of investigations must be maintained. Where a member of staff is under investigation for offences that could lead to dismissal and / or criminal charges, suspension from duty must be considered.

5.16 Insurance

The Trust insurance does not provide cover for items such as PCs, tablets, laptops and other associated equipment. If a computer is lost or damaged beyond repair, this must be reported to the IT Service Desk and Line Manager as soon as possible. Individual directorates may be responsible for funding a replacement.

6. Monitoring Compliance and Effectiveness

Trends relating to Information Technology and Cyber Security breaches received on incident report forms (IR1s) will be reported to the IGSG on a quarterly basis by the Head of IG. Subsequent action plans will be agreed by the IGSG.

Compliance with Information Technology and Cyber Security will be monitored against standards in the Data Security and Protection Toolkit. This is assessed three times a year and the assessments are subsequently submitted to the Department of Health.

The IGSG will monitor compliance with the toolkit on a quarterly basis. Where deficiencies are identified action plans will be developed and these will also be monitored by the IGSG.

7. References

NHS Care Records Guarantee (2009)

BS ISO/IEC 27002:2005

BS ISO/IEC 27001:2005 BS7799-2:2005

Department of Health (2007) Information Security NHS Code of Practice

Health and Social Care Information Centre – Principles of Information Security

Computer Misuse Act (1990)

Data Protection Act (2018) www.ico.org.uk

Public Interest Disclosure Act (1998)
www.legislation.gov.uk/ukpga/1998/23/contents

Appendix 1 - Information Technology & Cyber Security Incident – Procedure for Line Managers

Definition of an Information Technology Security Incident

A general definition of an Information Technology Security Incident would be the misuse of Information systems and the data held within these systems or the misuse of Trust IT equipment or services.

The following list is not exhaustive but is a guide to help identify the type of problems that would be seen as an Information Technology Security Incident:

- The use of a colleague's personal password to gain access to information. Inappropriate use of email
- Attempting to access, or successfully accessing pornographic, adult and other "unsuitable" sites
- Contravention of the Caldicott principles or Data Protection Act when accessing or handling confidential information
- Storing sensitive documents on a computer's desktop rather than storing onto the secured network (i.e. personal drive)
- Use of illegally copied software on Trust equipment or the unlicensed copying of official software either for private or Trust business, including copying Trust owned software
- Where investigations indicate or reveal mistreatment of children, this must be reported to the Trust Responsible Safeguarding Lead, Chief Executive and police.

Definition of a Cyber Security Incident

A general definition of a Cyber Security incident is an incident that threatens the security, confidentiality, integrity or availability of the Trusts information assets, information systems or networks that deliver those systems and disrupts the normal business of the Trust.

The following list is not exhaustive but is a guide to help identify the type of problems that would be seen as a Cyber Security Incident:

- A PC, laptop or server being infected with a computer virus or malware
- A PC, laptop or server being the target of a Ransomware attack
- A member of staff receiving and replying to a phishing attack
- The Trust's IT network being the target of a Denial of Service attack.

Action to be taken

1. General Information Technology or Cyber Security Incident

All Information Technology or Cyber Security incidents must be reported and investigated in line with the Trust Policy for Incident Reporting, Analysing, Investigating and Learning.

If a Line Manager suspects or is informed that an Information Technology Security Incident has occurred then the procedure below must be followed:

- Report the Incident to Head of IG and Head of IT
- The Line Manager must raise an IR1 and keep a full record of the actions taken including dates, times and personnel contacted.

If initial assessment deems the incident to be high risk:

- Inform the Divisional Quality Improvement Lead
- Do not investigate the incident by logging into systems or by checking software / files on the PC. This could corrupt evidence or compromise further disciplinary procedures. Await guidance from an IT Manager
- The details of the Incident will be reported to the Medical Director who will instigate an internal or external investigation in liaison with the Divisional Human Resources Business Partner (HRBP). No investigation will be undertaken without this permission
- If an incident is suspected out of hours, then it must be reported at the first opportunity on the next working day. Do not start the investigation until the Medical Director has approved an investigation to take place. Please remove the keyboard as a preventative measure as evidence may be destroyed if the correct procedure is not followed.

Investigation

If an investigation is required, then the appropriate Trust Board Directors will be notified by the Medical Director

- The Director of Workforce and Corporate Development will nominate a Human Resources Business Partner to form part of the Investigation Team.
- The Divisional Director will nominate the Senior Investigating Officer
- If an internal investigation is required the Investigating Team will be formed from a minimum of the Line Manager (Chair), Human Resources Business Partner and the Head of IT. This team must follow the Trust Disciplinary Policy and Trust Policy for Incident Reporting, Analysing, Investigating and Learning. If required, the Investigating Team will then decide whether logins and equipment should be secured. Where a serious offence is suspected the computer should be disconnected by a member of IT Services, in the presence of Human Resources and placed in a locked room. The access to that room must be permitted only by the relevant departmental or Head of IT. The equipment must not be set up or operated without two managers being present
- The Investigating Team must keep detailed records of actions taken and provide progress reports to the Medical Director. Equipment and evidence must be secured until approval is given by the Medical Director for re-use or disposal
- Following a disciplinary hearing, the Medical Director will advise on any restrictions for future use of IT systems.

External Investigation

If an external investigation is required, then the Trust Legal Advisor must be contacted by the nominated Human Resources Business Partner and the final decision to contact an external agency must be approved by the Medical Director. The Trust will then provide assistance and staff as requested by the external agency. The Human Resources Business Partner will ensure that the Trust Disciplinary Policy, Trust Policy for Incident Reporting, Analysing, Investigating and Learning are adhered to and that appropriate legislation is followed.

2. Serious Incident – Information Technology Security

The Head of IG and Head of IT will identify potential serious Incidents (SIs). An incident will be classified as a potential SI where:

- Actions of health service staff are likely to cause significant public concern
- Events might adversely impact upon the delivery of service plans and / or may reflect a serious breach of standards or quality of service
- It is an Information Governance incident graded 1-5:

    1. Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted.
    2. Serious potential breach & risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected.
    3. Serious breach of confidentiality. E.g. up to 100 people affected.
    4. Serious breach with either particular sensitivity. E.g. sexual health details, or up to 1000 people affected.
    5. Serious breach with potential for ID theft or over 1000 people affected.

The Head of IG and Head of IT will inform the Head of Patient Safety of any potential Serious Incidents. The Head of Patient Safety will highlight any potential SIs to the Executive Chief Nurse to be highlighted with the Executive Management Team, in accordance with the Policy for Incident Reporting, Analysing, Investigating and Learning.

3. Theft

Theft of IT equipment should be reported immediately to the Trust Security Department who will inform the police if required. Line Managers should also report incidents of theft to the IT Service Desk including as much detail as possible about data held on the equipment, exact location and any other information that would help when trying to identify the equipment.

The user and their Line Manager must complete an IR1 form, in accordance with the Policy for Incident Reporting, Analysing, Investigating and Learning, and keep a full record of the actions taken including dates, times and personnel contacted.

Appendix 2 - Backup Strategy for Trust managed systems

All live servers are backed up to tape on a nightly basis. These tapes are rotated on a weekly basis, every 4 weeks. Once a month, a complete set of backup tapes are removed from the weekly backup set and stored for a minimum of 2 years – these are known as ‘month end’ sets. All tapes that are not part of the current weekly set or are part of the month end sets are stored in a fireproof safe. The safe is in a separate fire zone to the computer rooms.

All file servers have a full backup taken once a week, on the other 6 days, a differential backup is taken (a differential backup is one that includes all files that have been modified since the last full backup). These backup jobs backup first to disk and then to tape to improve performance and backup time.

Database servers back up their database files to their own local disk storage every day. These files are then backed up to tape, ensuring the backup to disk has finished first.

Servers that have 3rd party applications on are backed up in accordance with instructions from the software suppliers, usually in the form of an email or official configuration documentation.

Test / Train servers are not backed up unless specifically requested.

Backup logs are checked daily by the server team who resolve any issues internally. Database backup logs are checked daily by the Clinical Systems team and escalated to the server team if necessary.

Appendix 3 – System and Audit Logs

1. Clinical Systems Logging

All clinical systems in use within the Trust retain an audit log of access and actions taken. The length of time this information is retained for varies from system to system, but the minimum period it is retained for on any system is 1 year. The clinical systems team are able to run queries on the logs, either directly or with the support of a third party.

All events are logged include the following standard data – date and time, event description, what activity was performed, what or who performed the activity and what the activity was performed one. This also includes access to any patient records.

How to request access to log file information

A request must be logged with the IT Service desk as a Sunrise call, approval is required from a Divisional Director. It is also be necessary to get authorisation from the HR department.

2. Windows Workstation and Server Logging

Within the Trust we have a number of systems that monitor users and workstations and log event information to log files. They contain information about usage and operations of operating systems, applications or devices.

These event logs can be used to monitor usage or investigate and troubleshoot performance issues. Event logs can also be used to track users, identify suspicious activity and detect vulnerabilities. Event logs will record events and monitoring these events can identify possible incidents.

Event logs must be kept for a minimum of 6 months.

Basic reporting can be carried out on all the systems below but for many of the event logs it will require specialist knowledge of the system and training on advanced reporting.

Source	**Description**	**Summary of Events reported**
Certero	Asset Management	Workstation and User events
Darktrace	Network Behaviour	Network device behaviour
SCCM	Software and patch distribution	Software installations and workstation patching
Smoothwall	Web Filter	Web browsing time and websites
Sophos	Antivirus	Application and USB devices allowed / blocked
Windows MDE formerly ATP	Threat Protection	Security scores, threats and vulnerabilities
Windows Server Event Logs	Application, database, System	Domain, Application events
WSUS	Automatic patching for Servers	Patches, installed, required and server status

Typical events that can be reported on and investigated within each system:

- **Certero** – hardware and software inventory, user accounts that have logged in to a device
- **Darktrace** – network behaviour and traffic monitoring, other devices contacted on the internal network
- **SCCM** – updates and Software installation on workstations
- **Smoothwall** – Internet browsing activity
- **Sophos** – blocked applications and USB devices
- **Windows MDE (formerly ATP)** - login events, user activity on a computer
- **Windows Server and Workstion Event Logs** - all workstations have Windows Event logs enabled by default. They are stored on the local disk of the machine and any user that can login locally can access the event viewer. Event Viewer can be used to access a remote computer if the appropriate user account is used
- **WSUS** – server patch levels, installed and needed patches and whether an update is approved for install

All events that are logged include the following standard data – date and time, event description, what activity was performed, what or who performed the activity and what the activity was performed on, the result of the activity – success / failure

How to request access to log file information

A request must be logged with the IT Service desk as a Sunrise call, approval is required from a Divisional Director. It is also be necessary to get authorisation from the HR department.