Trust-wide Document

Great Western Hospitals NHS Foundation Trust

Data Security & Protection Policy

Document No	Corp - 00255	**Version No**	4.0
Ratified by	Information Governance Steering Group	**Date Ratified**	14/06/2024
Date implemented (made live for use)	05/07/2024	**Next Review Date**	14/06/2027
Status	LIVE		
Target Audience- who does the document apply to and who should be using it. - The target audience has the responsibility to ensure their compliance with this document by: • Ensuring any training required is attended and kept up to date. • Ensuring any competencies required are maintained. • Co-operating with the development and implementation of policies as part of their normal duties and responsibilities.	All employees directly employed by the Trust whether permanent, part-time or temporary (including fixed-term contract). It applies equally to all others working for the Trust, including private-sector, voluntary-sector, bank, agency, locum, and secondees. For simplicity, they are referred to as 'employees' throughout this policy		
Special Cases	There are no special cases that do not apply to this document.		
Accountable Director	Director of Information Technology (IT)		
Author/originator – Any Comments on this document should be addressed to the author	Senior Information Governance Officer		
Division and Department	Corporate. Information Governance (IG) and IT		
Implementation Lead	Information Governance Manager		
If developed in partnership with another agency ratification details of the relevant agency	n/a		
Regulatory Position	Data Protection Act 2018 Freedom of Information Act 2000 Civil Contingencies Act 2004 Computer Misuse Act 1990 Copyright, Patents & Designs Act 1988 Crime & Disorder Act 1998 (Ref 12)		
Review period. This document will be fully reviewed every three years in accordance with the Trust's agreed process for reviewing Trust -wide documents. Changes in practice, to statutory requirements, revised professional or clinical standards and/or local/national directives are to be made as and when the change is identified.			

Contents

Instant Information - Background

In accordance with data protection laws, Great Western Hospitals NHS Foundation Trust (the Trust) has to be open and transparent with its employees patients and the public about the use of personal information that it holds. This includes providing clear communications about how this information is collected, used, stored and shared. The Trust has available on its external website three privacy notices – one for patients, one for children and one for employees.

If an employee receives an enquiry from a patient or member of the public, or would like to know more about how their own personal information is used, they should refer to the privacy notices in the first instance.

Under the UK General Data Protection Regulation (GDPR) [Ref 2] and the Data Protection Act 2018 (DPA), a data controller (that is to say an organisation that determines the purposes for which and the means by which personal data is processed) must appoint a Data Protection Officer (DPO). This person's role is to be involved properly and in a timely manner with all issues which relate to the protection of personal data. In this Trust, the person appointed to this role is the Head of Information Governance who may be contacted on: 01793 605675 or email: gwh.info.gov@nhs.net.

The Trust has set out this policy to ensure that there is adequate security for the information that is processed. Data Security and Protection is the responsibility of everybody, whether they are substantive, bank, agency, locum, volunteer, student or otherwise.

1 Introduction & Purpose

1.1 Introduction & Purpose

Information held in electronic and manual information systems within the Trust represents one of its most valuable assets, as systems proliferate and increased reliance is placed upon them. It is therefore essential that all computers, networks, records libraries and information contained within them are protected against the many threats which may compromise data, patient/employee privacy, and/or the overall service provision. The Trust and its employees have responsibilities and legal requirements to keep sensitive information safe, secure and confidential at all times.

This policy aims to ensure that Trust information systems and information stores are properly assessed for security, that confidentiality, integrity and availability are maintained, that employees are aware of their responsibilities, roles and accountability, and that there are procedures in place to detect and resolve information security breaches.

Key issues addressed by this policy are:

- Confidentiality – ensuring information is accessible only to authorised employees/users.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – information and associated assets are available to authorised users when required.
- Risk Assessment – assessing threats to, impacts on, and vulnerabilities of, information and information processing facilities and the likelihood of their occurrence.
- Risk Management – process for identifying, controlling and minimising/eliminating information security risks that may affect IT systems or other information assets.

1.2 Glossary/Definitions

The following terms and acronyms are used within the document:

ARAC	Audit, Risk and Assurance Committee
BCM	Business Continuity Management
CD-ROM	Compact Disc, read-only memory
CQC	Care Quality Commission
DBS	Demographic Batch Service (formerly NSTS)
DPO	Data Protection Officer
EIA	Equality Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
HSCN	NHS Health and Social Care Network (previously known as N3)
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IP&C	Infection Prevention and Control
IT	Information Technology
MFD	Multi-Function Device
MFP	Multi-Function Printer
NHS	National Health Service
PCs	Personal Computers
PDS	Patient Demographic Service
RAS	Remote Access Service
RBAC/PBAC	Role/position-based access
SIRI	Serious Incident Requiring Investigation
SIRO	Senior Information Risk Owner
UK	United Kingdom
UPS	Uninterruptable Power Supply
USB	Universal Serial Bus

2 Main Document Requirements

2.1 Objectives

The Trust's information security management system has the following objectives, which are to:

- Establish the management structure for the security of information systems within the Trust;
- Ensure that Trust employees are aware of information security risks and their responsibilities to minimise the threats;
- Protect IT equipment against loss or damage and avoid interruption to business activity;
- Enable the Trust to control external access to its computer systems;
- Detect, investigate and resolve any suspected or actual information security breaches;
- Identify the location of the Trust's IT assets and information assets and to authorise the use of such assets where appropriate;
- Minimise the threat to the Trust's information systems through damage or interference;
- Control individual access to systems by those employees with a need to know, as required by their job function;
- Maintain the integrity and availability of computer assets, including the monitoring for, and removal of, unsupported devices;
- Maintain confidence in data quality for use in decision-making;
- Comply with the law on licensed products and minimise the risk of computer viruses, worms, trojans and/or malicious code;
- Comply with the recommendations of the Caldicott Report (Ref 14)as required by the NHS Executive, GDPR (Ref 2) and the Data Protection Act 2018 (Ref 12), with regard to the proper collection, storage, processing and disclosure of person-identifiable data;
- Identify and counter possible threats to the security policy and standards;

- Monitor and act upon CareCERT cyber security threat notifications, bulletins and immediate high-severity alerts issued by the Data Security Centre, and NHS Digital;
- Conduct an annual penetration testing audit;
- Be able to maintain essential business services and activities, as far as practicable, during periods of breakdown or malfunction;
- Be able to restore computer facilities following a major failure or disaster;
- Ensure that relevant legislation is adhered to and that employees are aware of the implications.

Details of how these objectives are met is contained in the following sections.

2.2 Information Security Management

2.2.1 National Information Security Management

NHS Digital manages and monitors the day-to-day delivery of key national systems and services; approves and accredits local and national IT systems against technical and clinical safety standards so that information can be shared safely; and supports the delivery of information standards and governance.

2.2.2 NHS Health & Social Care Network (HSCN)

HSCN, the NHS national network, is recognised by NHS employees, the Department of Health and Social Care and Government as a successful and indispensable part of national and local IT services. In order to obtain a connection to HSCN, third party organisations must complete an application process via NHS Digital which includes the HSCN Connection Agreement and involves being “sponsored” by an NHS organisation. Once the application is successful, NHS Digital will send the third party organisation an Organisational Data Services (ODS) Code and log-in code. This will enable them to complete a Data Security and Protection Toolkit assessment, to be submitted annually.

Third party suppliers are also required to implement specific security measures, such as appropriate fire-walling of external connections, vigorous measures for virus protection, and access control. These security measures apply to all systems and users connected to the Trust’s network. Security incidents and breaches must be reported centrally via the Trust’s incident reporting system.

2.2.3 Auditors

Security controls implemented on Trust systems are to be reviewed periodically by the Trust’s independent internal auditors, as part of the agreed audit programme covering the IT department. Audit recommendations are normally to be implemented unless specific dispensation is given at Trust management level.

2.3 Information Risk Management

2.3.1 Information Asset Management

Information assets such as systems and record libraries are to be owned on behalf of the Trust by an Information Asset Owner (IAO) and administered by an Information Asset Administrator (IAA). The IAO is to be the senior manager who authorises the collection, storage and use of the data held in the asset. The IAA is to be the employee with day-to-day operational responsibility for the management of the asset and the security of the data held. The IAO is responsible for ensuring that the asset’s information risk is periodically assessed, with input and support from the IAA as necessary, and with advice from the IT department and Information Governance team. Please refer to the Information Asset Risk Management Policy (Ref. 1) for further details.

2.3.2 Methodology

The IAO is to ensure that the security of the information asset(s) for which they are responsible is reviewed at least annually. The security and risks will be documented in the assessment form. The depth of the review should be determined by the business criticality and extent of usage of the particular

asset. As a minimum, the IAO will confirm annually whether the information in the assessment form is correct and up-to-date, providing new information where required.

Reviews are to include:

- General management of the system; such as the type of data processed, location of the system/server, software used, support and maintenance arrangements, business continuity planning, quantity of data and how critical the system is to the organisation;
- Access control; including password management, audit trail functionality, role/position based access control (RBAC/PBAC), SMARTcard access and tiered access such read only.

Aims of the security assessments:

- Identification of all significant components of the information asset;
- Evaluation of potential threats;
- Assessment of likelihood of threats occurring;
- Identification of practical cost-effective controls and counter measures;
- Action plan for implementing controls and counter measures.

The resultant risk assessments and risk treatment plans may be recorded against the asset on the Information Asset Register, and any exceptional risks will be reported to the Trust's Senior Information Risk Owner (SIRO).

2.3.3 New Software

A process of authorising new software is to be used, to assess its suitability for integration with the Trust's current systems, the data quality of information within the system, and to ensure that the software meets appropriate security guidelines. Trust departments are to seek the advice and assistance of the IT Department (IT Projects team) when considering the procurement and implementation of any new systems/software.

Where a Trust department is considering a new business process or a new system, the relevant business manager (or the prospective IAO of the asset) is to ensure that a Data Protection Impact Assessment (DPIA) is conducted to identify any potential issues with security, data protection and confidentiality. Please refer to the Data Protection Policy (Ref 9) for further information. This must be completed at the earliest opportunity in the project to ensure that processes being implemented do not have a detrimental impact on the privacy of our patients and/or employees.

2.4 Asset Control

2.4.1 Physical Assets

A register of acquisitions and disposals of physical computer assets is to be maintained. The registered details are to include the location, serial number and specification of the asset. This register is normally maintained by the IT Department. The value of the asset is not held on an individual asset basis but on a global funding basis. Separate registers may be used for different types of assets, e.g. Personal Computers (PCs), telephony equipment, network/infrastructure equipment. There are also separate registers/logs of medical equipment used within the Trust which are managed by, and the responsibility of, the Medical Equipment team.

2.4.2 Software Assets

A register of all proprietary software must be maintained to ensure that the Trust is aware of its assets and that licence conditions are followed. This register is to be maintained by the IT Department. Licences are kept and stored manually.

2.4.3 Information Assets

A register of all significant information assets is to be maintained in accordance with the Information Asset Risk Management Policy (Ref. 1). The registered details are to include the names of the Information Asset Owner (IAO) and the Information Asset Administrator (IAA), an assessment of the associated information risk, and a description of any specific Business Continuity Management (BCM) measures.

2.5 Software Protection

2.5.1 Licensed Software

All users must ensure that they use only licensed copies of software as permitted by the IT Department. It is a criminal offence to make or use unauthorised copies of commercial software and offenders may be subject to disciplinary action.

The Trust uses NHS mail and where applicable to the employee's job role, they will be provided with an NHS mail email account. NHS Digital, the owners of the NHS mail system, permits use of the system for some non-work activities. This is only allowed in accordance with their terms and conditions of use and must never interfere with Trust activities. See the NHS Mail Terms and Conditions available from the NHS mail website - NHSmail 2 Portal - Home and the Trust's Internet and Email Usage Policy (ref 15) for further information.

2.5.2 Trust Software Standards

The Trust permits only approved software to be installed on its devices. Approval is to be obtained via the IT Department and is required in advance of any usage

The Trust requires the use of specific general-purpose computer packages (e.g. word-processing, spreadsheets, and databases) to facilitate employee training, support and flexibility.

Where the Trust recognises the need for specific specialised computer products, each installation of such approved products must be registered with the IT Department and be fully licensed.

2.5.3 Virus Control

The Trust seeks to minimise the risks of computer viruses, worms, trojans and/or malicious code through education, good practice, procedures, anti-virus software and firewalls.

The Trust has deployed anti-virus and anti-malware software to all GWH IT Controlled Assets and there are automatic updates set in the implementation policy.

The requirement to have anti-virus software installed is also detailed in the Internet and Email Usage Policy (ref 15), which covers downloading of information and software installation. Auto-run is also disabled by default.

The Trust's virus protection includes endpoint security with the following Threat Detection Capabilities:

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)
- File reputation
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- DLP

- Device control
- Good file check
- Sandbox and breach detection integration
- Detection and response
- Endpoint encryption (requires separate agent)
- Vulnerability protection

Protect Data at Rest, In Use, and In Motion
The Trust's package recognises and processes over 300 file types, including most email and office productivity applications, programming languages, graphics, engineering files, and compressed or archived files. Discovery capabilities scan the endpoint, file server, MailStore, Microsoft© SharePoint© Portal Server repository, including SaaS applications and cloud storage, to see where compliance data is located.

The package offers visibility and control of data in motion - whether it's in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP.

The package offers visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems. It can also be configured to monitor copy and paste and print screen.

The Trust maintains a list of types of website which cannot be accessed. If a user requires access to one of these sites, then they must put a request into the IT Service Desk, who will request advice from the IG team.

As users of NHS mail, the Trust benefits from Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) to make email spoofing difficult. In addition, NHS mail has spam and malware filtering, and enforces DMARC on inbound email. Spam emails which are received can be blocked or reported to spamreports@nhs.net.

Users must report any viruses, worms, trojans and malicious code detected or suspected on their computers immediately via the IT Service Desk.

Any newly-acquired disk or other storage device/media – from whatever source – is not to be loaded onto a device unless it has previously been scanned by a locally-installed virus-checking package and has been reported to be virus-free.

2.6 Security of Equipment

2.6.1 Equipment Siting and Protection

IT equipment must always be installed and sited in accordance with the manufacturer's specification. Equipment must always be installed by, or with the permission of, the IT Department (this includes the attachment of PCs , laptops or devices to the network).

Where appropriate, environmental controls are to be installed to protect central or key equipment. Such controls trigger alarms if environmental problems occur. In such cases, where equipment is sited in a secure area, only authorised entry is to be permitted.

Employees must not eat, drink or smoke in these key areas, and doors must be kept closed at all times.

2.6.2 Power Supplies

In key locations, where the Trust has generator power as back-up to the mains electricity supply, key or critical computer equipment is to be covered by an Uninterruptable Power Supply (UPS) to ensure against failure during switchover between mains and generator.

2.6.3 Cable Routing

All electric cabling (power or communications) within buildings is in conduits if surface mounted, otherwise within the framework of the building. Cabling between separate buildings on The Great Western Hospital site is via underground conduit which is not accessible to unauthorised persons.

2.6.4 Equipment Maintenance

The IT Incident & Disaster Recovery Plan (Ref. 3) covers the maintenance of all servers. Some servers are covered by third party maintenance; others are custom-built and supported internally. There are surplus components available to support these servers.

There is a computer refresh programme that aims to adopt a five-year refresh cycle. Computers are purchased with standard three-year warranties and any breakdowns in the remaining period of use is covered by central funds.

The Great Western Hospital Site
The Trust has a managed print service arrangement for Multi-Function Devices (MFD), Multi-Function Printers (MFP) and single function printers, as supplied under contract. The devices are supported and maintained by the managed print service supplier, with equipment repairs, parts and replacement all included during the term of the contract that covers the GWH Campus and Community sites

Records of all faults or suspected faults must be maintained by the IT Service Desk on the Service Desk call-logging system.

2.6.5 Data Storage on Hard Disk Drives

Trust-owned data, especially all sensitive/confidential data, must be kept on secure network storage and not on the hard disk of a user's PC or other device. Unlike network storage, the hard disk of the user's PC or laptop is not accessible when using the Remote Access Service (RAS), and is not backed up – therefore data loss would occur in the event of a hard disk failure.

Information relating to individual employee management (e.g. appraisals, training certificates, sickness absence forms, expenses forms, timesheets etc.) should normally be kept on the private network storage of the employee or manager (the U: drive). Information relating to ordinary work matters (e.g. patient information, employee rotas, task lists, action plans, reports, correspondence etc.) should normally be kept on a shared network drive, where it will be available to team colleagues who may have a need to access it.

Network storage is provided by server systems containing hard disks. To remove such disks off-site (e.g. for specialist examination or repair) represents a potential threat to the Trust and patient/employee confidentiality. Each case is to be judged on its own merits, balancing the need versus the risk of breach of confidentiality. Where the disks are to be removed off-site, they must be sent by a secure method, and must be given to approved repairers who have signed confidentiality agreements. Whenever possible the data on the disks is to be overwritten using appropriate sanitising software. Hard disks must be destroyed in accordance with the guidelines in section 3.6.8 below.

2.6.6 Security of Equipment on Trust Premises

All Trust-owned desktop PCs located in high-risk areas and all Trust-owned laptops must have their hard disks encrypted in accordance with NHS guidelines. Security tethering cables are to be used in areas where the risk of theft is deemed higher.

2.6.7 Security of Equipment off Trust Premises

Trust-owned equipment and data must not be taken off-site, unless the employee has been authorised to work at home or to transport it between the Trust's sites. In these circumstances, the device holding the data must be encrypted. Line managers need to ensure their employees are aware of Trust security policies and that all data on portable devices (laptops, USB keys, tablets and Trust-owned Smartphones) are encrypted.

Portable computers (e.g. laptops) and other mobile equipment are vulnerable to theft, loss or unauthorised access, particularly if such a computer has network access capability. All Trust-owned laptops have been encrypted in accordance with NHS guidelines. To preserve the integrity of any data held on those portable computers, frequent transfers of data must be made from those devices onto network storage areas or Trust systems. Portable devices must be maintained regularly and any batteries kept charged to preserve their availability. Portable devices stored at home during periods of home-working must be kept in a secure place, away from other people in the household and must never be stored in places which are susceptible to theft, such as in cars.

2.6.8 Disposal of Equipment

All disposal of Trust-owned computer hardware must be authorised by the IT Department. The IT Department must ensure that data storage devices (e.g. hard disk drives, Universal Serial Bus (USB) memory sticks) are purged of all data before disposal or secure destruction.

Any unusable computer media must have the data erased if possible before being destroyed physically (e.g. floppy disks, magnetic tapes, Compact Disc, read-only memory (CD-ROMs)).

Please refer to the IT Equipment Usage Policy (Ref. 4) for further information.

2.7 Access Control to Secure Areas

2.7.1 Physical Security

All central processors, networked file servers and central network equipment must be located within restricted access areas. These areas are to be protected by security measures to restrict access by means of swipe cards, keys or keypad entry.

2.7.2 Entry Controls

Access is restricted to designated employees whose job function requires access. This is controlled by the Head of IT Operations. Restricted access may be given to other employees accompanied by designated employees where there is a specific job function or need for such access. Authenticated representatives of third-party support agencies must only be given access through specific authorisation from designated employees.

2.8 Entry Controls

2.8.1 Registering Users

Formal procedures must be used to control access to systems. An authorised manager must countersign each application for access – this can be done via email. For Smartcards, only approved officers within the Registration Authority can assign roles to the respective user's card. Access privileges must be modified or removed, as appropriate, when an individual changes job or leaves. It is the responsibility of the line manager to notify the IT Service Desk of any changes in employment using the relevant forms available from the intranet. This service is maintained by the IT Service Desk which administers access to the Trust's systems.

2.8.2 User Password Management

An employee must not be given access to a system unless properly trained and made aware of their responsibilities towards information security. Users must keep their passwords secret and never disclose them to colleagues or others. Passwords are to be changed regularly – all new systems must include password ageing to force users to change their password periodically.

Users with authorised access to more than one system may have the same password on all systems to which they have access. Any service/system that uses the PC/Windows logon name and password will require that:

- The password must be at least 8 characters in length
- It must also contain characters from three of the following four categories:
  - English UPPERCASE characters (A –Z)
  - English lowercase characters (a – z)
  - Base 10 digits (0 – 9)
  - Non-alphabetic characters (e.g. ! $ # %)

In addition to the password convention listed above, all users must ensure that:

a) They avoid choosing obvious passwords – for example, avoid using dates of birth, family names, pet's names or sports teams which might be known to others (or targeted through phishing emails)
b) They do not choose common passwords – for example, do not use 'Password123' or 'Pa55word' or other things which are common or guessable
c) They avoid repeating the same password over again. As mentioned in the previous section, the same password can be used for multiple systems if it is secure, but this must be changed regularly and not changed back to what it was previously
d) If any passwords hints have been written down (this is not recommended) that they are stored securely, in one single place (not duplicated) and not stored where the systems can be accessed. E.g. do not keep a file on the desktop which reminds you what the password is to Medway (accessible on the desktop)
e) They only use Trust-approved password management software such as the Single sign-on or Imprivata
f) passwords to clinical systems and/or cloud systems are never written down or recorded anywhere electronically (except using the approved password management software).

It is strongly recommended that the same password convention is applied to all other Trust systems containing personal and/or sensitive personal data.

2.9 Security of Third-Party Access

2.9.1 Access Control

No external agency (NHS or other) is to be given access to any of the Trust's networks unless that body has been formally authorised to have access. Normally this approval will be via an application form, with sponsorship from a senior manager and approved by the Clinical Records Group, or there will be a formal contract in place, for example with a supplier of an IT system. All non-NHS agencies must sign security and confidentiality agreements with the Trust. Standard forms are available on the Trust's intranet or on request from the Information Governance team.

Authorisation checks should include (where applicable) confirmation of the third-party need to know, adequacy of contractual clauses (concerning data protection, confidentiality, data quality and freedom of information) and due diligence checks completed by the IG team which includes, compliance with ICO requirements for Data Controller registration, submission of Data Security and Protection Toolkit assessments, certification to ISO/IEC 27001/27007, Cyber Essentials and Cyber Essentials Plus accreditation. Any serious incidents reported to the ICO will also be recorded. The IG team will keep this information on the due diligence log and updated annually.

The Trust must control all external agencies' access to its systems by enabling and disabling connections for each approved access requirement, or by accompanying them if on a site visit.

2.9.2 NHS Health & Social Care Network (HSCN) Requirements

Strong authentication procedures and technology must be implemented for all dial-up connections to the Trust's computer systems where concurrent connection to HSCN is possible.

The HSCN network allows connection via strong authentication to the Trust's computer systems from the internet. Please refer to the Remote Access for Employees and Third Parties Policy (Ref. 5) for further information.

2.9.3 Remote Diagnostic Services

Suppliers of central systems and software expect to have remote access to such systems on request to investigate or fix faults. The Trust will only permit such access if it is initiated by the system supplier and actively monitored. The default access method is to be via an HSCN connection, rather than by remote access service (RAS) or dial-up connections.

Each supplier requiring remote access must commit to maintaining confidentiality of data and information and use only qualified representatives.

Where a third-party organisation has been authorised to access the Trust's networks/data, a separate request must be submitted each time that remote access is required for diagnostic services. Each request for remote access must be authorised by approved IT Department employees, who are to make the connection only when satisfied of the need. Strong authentication methods must be used. These methods are to be reviewed periodically to ensure that best practice is being followed. The connection must be physically broken when the fault has been fixed or when the supplier ends its session.
Please refer to the Remote Access for Employees and Third Parties Policy (Ref. 5) for further information.

2.10 Data Quality

2.10.1 Data Validation

Data accuracy is the direct responsibility of the person inputting the data, who is to be supported by their line manager.

All systems must include validation processes at the time of data input to check, in full or in part, the acceptability of the data. Depending on the system, later stages of validation are also to be carried out, where necessary, in order to maintain referential integrity.

Systems are to report all validation errors together with a helpful reason for the rejection to facilitate data correction.

Error correction is to be done at the source of data input as soon as it is detected, or the error is to be reported to an appropriate employee for correction, where responsibility for this has been limited to key individuals. Error detection and correction are increasingly important as systems are linked and errors can be transmitted between systems.

Any loss or corruption of data must be reported to the IT Service Desk at once – this is to involve incident recording mechanisms immediately and possibly major incident control (dependent on the severity of the problem).

2.10.2 Internal Validation

Systems are to incorporate internal validation processes and audit trails to detect and record problems with processing or data integrity.

2.11 Data Exchange

2.11.1 Safe Havens

Arrangements must be made to provide designated contact points through which confidential information is to pass when being transferred from organisation to organisation. These must encompass the transfer of physical documents, faxes, and disclosures by telephone. For more information and guidance please refer to the Information Governance Policy (Ref. 6).

2.11.2 Protocols

All routine flows of information to/from external organisations (such as other NHS Trusts and healthcare providers, social, welfare and education services, voluntary and private sector providers) are to be identified, and protocols governing the secure transfer of information are to be developed and agreed. This process is to be continuous in respect of any new flows of information which come into being.

There are to be generic processes in place to deal with non-routine or one-off disclosures, for which the Information Governance team is to be notified. These processes are to include the agreement and documentation of the method of transfer of information, the purposes for the transfer, and the specific security arrangements under which the information shall be transferred, stored and used. Further information and the appropriate forms can be found in the Information Governance Policy (Ref. 6).

2.11.3 Patient Demographic Data

There are two principle NHS tools used to provide NHS Trusts with patient demographic data – the Patient Demographic Service (PDS query tool) and the Demographic Batch Service (DBS batch tool). Together they can provide a core set of administrative information about people, places and organisations, including the ability to call up the full range of administrative details for an individual.

Each employee with a need to access PDS and/or DBS is to be authorised and assigned an access profile by the designated authorities for PDS and DBS within the Trust, on behalf of the Caldicott Guardian.

2.12 Information Security Incident Management

2.12.1 Information Security Incidents

An information security incident is an event, which may result in:

- Disclosure of confidential information;
- Unauthorised access to applications;
- Degraded system integrity;
- Significant loss of system availability;
- Disruption of activity;
- Financial loss;
- Legal action.

Incidents must be reported on the Incident management system (using an incident notification form). Where necessary the Information Governance team is to report incidents to external agencies. Refer to the Data Security and Protection Incident Reporting Procedure (Ref. 7). Information security breaches by employees may result in disciplinary action.

2.12.2 Logging Information Security Incidents

All information security incidents or issues must be formally logged as described in the Trust's Data Security and Protection Incident Reporting Procedure (Ref. 7). These incidents are categorised by significance and severity, and the associated actions and resolution are recorded. The IT Service Desk must be informed of information security incidents or issues which are to be logged onto its call-logging system. Employees wanting to speak to someone in confidence can contact the Information Governance team. The incident must be reported to the relevant technical or managerial employees and when necessary a Trust incident report form is to be completed.

Where an incident involves personal information, it may be classified as a Serious Incident (SI) and it may need to be reported to external bodies such as NHS Digital and the ICO.

2.13 Disaster Recovery Planning

2.13.1 Need for Effective Plans

The Trust recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core business via the IT Incident & Disaster Recovery Plan (Ref. 3) and related documents.

The Trust recognises that IT systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms.

2.13.2 Planning Process

The main elements of this planning process include:-

- Identification of critical computer systems;
- Identification and prioritisation of key users/user areas;
- Agreement with users to identify disaster scenarios and what levels of disaster recovery are required;
- Identification of areas of greatest vulnerability based on risk assessment;
- Mitigation of risks by developing resilience;
- Developing, documenting and testing disaster recovery plans including the identification of tasks, agreeing responsibilities and defining priorities.

2.13.3 Planning Framework

The IT Incident & Disaster Recovery Plan (Ref. 3) caters for different levels of incident including:-

- Loss of key user area within a building;
- Loss of a key building;
- Loss of key part of computer network;
- Loss of processing power.

The plan includes:-

- Emergency procedures covering immediate actions to be taken in response to an incident (e.g. Alerting disaster recovery personnel);
- Fallback procedures describing the actions to be taken to provide contingency devices defined in the disaster recovery plan;
- Resumption procedures describing the actions to be taken to return to full normal service;
- Testing procedures describing how the disaster recovery plan is to be tested.

2.14 Housekeeping

2.14.1 Data Back-Up

The Trust's back-up strategy is detailed in the IT Back-up Strategy document (Ref. 8). The current back-up approach is designed to minimise data loss through the use of industry standard software aligned with a two-stage back-up process using both disk and tape.

2.14.2 Controlled Stationary

Examples of controlled stationery include payment stationery, drug ordering forms and prescriptions.

Formal procedures are to be established to control and account for the use of such stationery. Each type of stationery is to be assigned a unique identifier to assist the control and management of the stationery. Procedures are to be maintained within each relevant department.

2.14.3 Media Disposal

Disposal of removable media is covered under section 3.6.8 above.

2.15 Compliance with Legislation

2.15.1 Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR)

In order to comply with the Data Protection Act 2018, the Data Protection Officer (DPO) must ensure that the Trust keeps records of all personal data processed by the Trust and makes the appropriate notifications to the Information Commissioner's Office. Please refer to the Data Protection Policy (Ref. 9) for further details.

Each data set may be subject to review to ensure compliance with the Data Protection Act, UK GDPR and the Caldicott Principles.

The Trust's overall compliance with the Data Protection Act is assured by means of the Data Protection Policy (Ref. 9).

2.15.2 Copyright, Designs and Patents Act 1988

In order to comply with this legislation as regards use of software, Trust employees must adopt the procedures set out in section 2.5 above.

2.15.3 Computer Misuse Act 1990

Trust employees and any third party users must be made aware that access to systems is not permitted except where this has been formally authorised and documented.

The Trust must make arrangements to ensure that any offences under this Act can be proven by the use of appropriate sign-on messages and the logging of all major accesses and modifications to Trust data.

2.15.4 Freedom of Information Act 2000

The Freedom of Information Act Publication Scheme (Ref. 10) is available on the Trust's internet website. This identifies the information and documents which are routinely published by the Trust.

Other information is available, subject to any exemptions under the Act, on request to the lead manager for Freedom of Information in the Information Governance Team.

3 Monitoring Compliance and Effectiveness of Implementation

The arrangements for monitoring compliance are outlined in the table below: -

Measurable policy objectives	Monitoring or audit method	Monitoring responsibility (individual, group or committee)	Frequency of monitoring	Reporting arrangements (committee or group the monitoring results is presented to)	What action will be taken if gaps are identified
Assessment of the Trust's performance and evidence against Data Security and Protection Toolkit requirements	On-line assessment	IG Team	Annually	IGSG and Audit, Risk and Assurance Committee (ARAC)	Detailed action plan maintained by the IG Team for each year's IG Toolkit assessment.
Independent in-year review of IG compliance and assurance	Audit of IG Toolkit assessment and evidence; report with action plan	Trust's internal auditors	Annual	IGSG and ARAC	Action plan in audit report updated by IG Team.
Overview of past IG progress and future IG plans	Annual Information Governance Report	Director of IT	Annually	IGSG and ARAC	ARAC action plan for remedial work required.
Programme of IG work in the current year	Annual IG Work Programme	IG Manager	Annual revision and quarterly progress update	IGSG	IGSG action plan for remedial work required.
Review of IG action plans and progress	Action plan attached to IGSG agendas/minutes	IG Team	At monthly IGSG meetings	IGSG	IGSG to specify amended actions.
Review of IG incidents	IG incident reports	IG Team	Monthly and half-yearly reports	IGSG	IGSG action plan for remedial work required.
Review of IG compliance at departmental level	IG Checklists (separate versions for clinical & corporate depts.)	IG Team	At least twice per year	IGSG	IG Team to act on individual returns; IGSG action plan for remedial work re

					areas of concern.
Programme of auditing access to clinical systems	Summary report of monthly audits	IG Team	Annually	IGSG and Patient Records Committee	IGSG action plan for remedial work required.
Review of Subject Access requests	Summary report of statistics and trends	Health Records Manager	Quarterly	IGSG	IGSG action plan for remedial work required.
Review of FOI requests	Summary report of statistics and trends	IG Team	Quarterly	IGSG	IGSG action plan for remedial work required.
Public reports on IG, IG-related incidents and information risk management	Trust Annual Report including the Annual Governance Statement (AGS)	IG Manager, SIRO and Head of Governance	Annually	IGSG	IGSG action plan for remedial work required.
Information Asset / System Security Assessments	Assessment tool and summary report approved by SIRO	IG Team	Annually	Information Governance Steering Group – final approval by SIRO	IGSG action plan for remedial work required
Annual penetration testing audit	Audit report and action plan	Director of IT	Annually	IGSG and ARAC	ARAC action plan for remedial work required.

4 Duties and Responsibilities of Individuals and Groups

4.1 Chief Executive

The Chief Executive is ultimately responsible for the implementation of this document.

4.2 Ward Managers, Matrons and Managers for Non Clinical Services

All Ward Managers, Matrons and Managers for Non Clinical Services must ensure that employees within their area are aware of this document; able to implement the document and that any superseded documents are destroyed.

4.3 Document Author and Document Implementation Lead

The document Author and the document Implementation Lead are responsible for identifying the need for a change in this document as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and resubmitting the document for approval and republication if changes are required.

4.4 Management Responsibilities

It is the responsibility of managers to ensure the following, with respect to their employees:

- Employees are to be made aware of their responsibilities as regards information security.
- Employees using information systems/media are to be trained in their use.
- Employees are to be made aware of the consequences of permitting unauthorised access to any of the Trust's information systems, thereby compromising data security, integrity and availability.
- Employees are to be authorised to access specific information systems according to the requirements of their job function, independent of their status within the Trust.
- Procedures are to be implemented to minimise the Trust's exposure to fraud, theft, or disruption of its systems, particularly in critical susceptible areas, by means such as the segregation of duties, dual control, or employee rotation.
- Current documentation is to be maintained for all critical job functions to ensure continuity in the event of employee unavailability.
- Employees are to be made aware of Trust's Standing Orders on potential personal conflicts of interest.
- Employees must sign confidentiality (non-disclosure) undertakings as part of their contract of employment and have read and understood the Information Governance Policy (Ref. 6).
- The manager is to advise the IT Service Desk immediately of any changes affecting computer access (e.g. job function changes, redeployment to another department, or leaving the Trust) so that systems access may be amended or withdrawn.
- Each contractor or temporary worker undertaking work for or on behalf of the Trust must sign a confidentiality (non-disclosure) undertaking.

4.5 Employee Responsibilities

Employees are responsible for ensuring that no information security breaches or unwarranted disclosure of information result from their actions.

Employees must not share or disclose passwords and must inform their line manager, the IT Service Desk or the Information Governance team if they think a breach may have occurred.

Employees must declare any potential conflicts of interest as required by the Managing Conflicts of Interest in the NHS Policy (Ref. 11).

All employees must complete annual information governance training, including the induction assessment upon starting at the Trust and the refresher module in every subsequent year. A training needs analysis has been completed to determine the level of training required for different employee groups and is approved annually by the IG Steering Group.

4.6 Caldicott Guardian

The Trust is required to nominate a senior clinician to act as Caldicott Guardian and oversee various issues related to the confidential usage of patient information. The Trust has nominated the Medical Director to act as Caldicott Guardian and the Deputy Medical Director to act as Deputy Caldicott Guardian.

4.7 Senior Information Risk Owner (SIRO)

The Trust is required to nominate an employee of Board level to be accountable for the organisation's information risk. The Trust has nominated the Director of Finance to act as SIRO and the Deputy Director of Finance to act as Deputy SIRO.

4.8 Information Governance Team

The Information Governance team has responsibilities for:

- Monitoring and reporting on the state of information security within the Trust;
- Developing and enforcing detailed procedures to maintain information security;

- Ensuring that this policy remains compliant with relevant legislation;
- Ensuring that Trust employees are aware of their responsibilities for information security;
- Monitoring actual or potential information security breaches;
- Managing the handling and reporting of information security incidents.

4.9 IAO and IAA Responsibilities

Overall responsibility for particular information assets (e.g. systems and record libraries) rests with the relevant Information Asset Owner, with support from the Information Asset Administrator and advice from the IT department and the Information Governance Team. Please refer to the Information Asset Risk Management Policy (Ref. 1) for further details.

4.10 IT Department Responsibilities

The Head of IT Operations is responsible to the Director of IT for:

- Compliance of Trust-controlled systems with NHS security guidelines;
- The secure and safe storage of data on Trust servers;
- Managing the Trust's IT security protection facilities;
- Developing Trust-wide IT security and usage policies.

The IT Department is to have at least two or three employees with the necessary technical expertise to control and administer each of the Trust's more critical IT systems.

5 Further Reading, Consultation and Glossary

5.1 References, Further Reading and Links to Other Policies

The following is a list of other policies, procedural documents or guidance documents (internal or external) which employees should refer to for further details:

Ref. No.	Document Title	Document Location
1	Information Asset Risk Management Policy	Intranet
2	UK General Data Protection Regulation (GDPR)	https://ico.org.uk/
3	IT Incident & Disaster Recovery Plan	T:\Trust-wide Documents
4	IT Equipment Usage Policy	T:\Trust-wide Documents
5	Remote Access for Employees and Third Parties Policy	T:\Trust-wide Documents
6	Information Governance Policy	T:\Trust-wide Documents
7	Data Security and Protection Incident Reporting Procedure	T:\Trust-wide Documents
8	IT Backup Strategy	T:\Trust-wide Documents
9	Data Protection Policy	T:\Trust-wide Documents
10	Freedom of Information Publication Scheme	Trust Internet website
11	Managing Conflicts of Interest in the NHS Policy	T:\Trust-wide Documents

Ref. No.	Document Title	Document Location
12	• Data Protection Act 2018 • Freedom of Information Act 2000 • Civil Contingencies Act 2004 • Computer Misuse Act 1990 • Copyright, Patents & Designs Act 1988 Crime & Disorder Act 1998	www.legislation.gov.uk
13	• Confidentiality: NHS Code of Practice • Information Security Management: NHS Code of Practice • NHS Information Governance – Guidance on Legal and Professional Obligations	www.gov.uk
14	• Caldicott Report	https://www.gov.uk/government/publications/the-information-governance-review
15	• Internet and Email Usage Policy	T:\Trust-wide Documents

5.2 Consultation Process

The following is a list of consultees in formulating this document and the date that they approved the document:

Job Title / Department	Date Consultee Agreed Document Contents
Head of IT Operations	2 June 2024
Chief Clinical Information Officer	7 June 2024
Senior IG Officer	4 June 2024

6 Equality Impact Assessment

An Equality Impact Assessment (EIA) has been completed for this document and can be found at Appendix A.

Appendix A - STAGE 1: Initial Screening For Equality Impact Assessment

At this stage, the following questions need to be considered:			
1	What is the name of the policy, strategy or project? Data Security and Protection Policy		
2.	Briefly describe the aim of the policy, strategy, and project. What needs or duty is it designed to meet? The Trust has set out this policy to ensure that there is adequate security for the information that is processed. Data Security and Protection is the responsibility of everybody, whether they are substantive, bank, agency, locum, volunteer, student or otherwise.		
3.	Is there any evidence or reason to believe that the policy, strategy or project could have an adverse or negative impact on any of the nine protected characteristics (as per Appendix A)?		**No**
4.	Is there evidence or other reason to believe that anyone with one or more of the nine protected characteristics have different needs and experiences that this policy is likely to assist i.e. there might be a *relative* adverse effect on other groups?		**No**
5.	Has prior consultation taken place with organisations or groups of persons with one or more of the nine protected characteristics of which has indicated a pre-existing problem which this policy, strategy, service redesign or project is likely to address?		**No**

Signed by the manager undertaking the assessment	M Arnold
Date completed	04 July 2024
Job Title	Head of Information Governance and DPO

On completion of Stage 1 required if you have answered YES to one or more of questions 3, 4 and 5 above you need to complete a STAGE 2 - Full Equality Impact Assessment

Appendix B – Training Needs Analysis (TNA)

Staff Group	Induction	Non-clinical IG Refresher training	IG Refresher Training	Information Risk and Security Training	Caldicott Training	Information Risk, Cyber Security and Accountability
Bank staff	✓		✓			
Board – including Non-Executive Directors	✓		✓			✓
Caldicott Guardian	✓		✓		✓	
Clinical Admin	✓		✓			
Clinical staff (All)	✓		✓			
Corporate teams with access to Trust or patient data – e.g. Finance, Procurement, IT, Medical Records, etc.	✓		✓			
Corporate teams with **NO** access to Trust or patient data – e.g. Catering, Estates and Facilities, Portering, etc.	✓	✓				
IAOs / IAAs	✓		✓	✓		
SIRO	✓		✓	✓		✓
Volunteers	✓		✓			