Digital Acceptable Use Policy

This document describes the controls, processes and risk management put in place to maintain the confidentiality, integrity and availability of information stored and processed on Leicestershire Partnership NHS Trust IT infrastructure

Key words: IT, cyber, information, security

Version: 1

Approved by: Data Privacy Group

Ratified By: Finance and Performance Committee

Date this version was ratified: April 2025

Date issued for publication: 20th May 2025

Review date: 1 March 2026

Expiry date: 30 September 2026

Type of Policy: Clinical and non-clinical.

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

Contents

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

Policy On A Page

SUMMARY & AIM

The aim of this policy is to establish an overarching framework, outlining the approach, methodology and responsibilities for Information security and risk that provides assurance that:

- Members of staff are aware of their responsibilities concerning security of IT resources and confidentiality of information they use, and that information security is an integral part of their day-to-day business.

KEY REQUIREMENTS

For quick reference the guide below is a summary of the expectations of this policy. This does not negate the need for all staff to be aware of the detail outlined but is intended to assist staff in understanding their roles and responsibilities at a glance.

- You are personally responsible for ensuring that no actual or potential security breaches occur as a result of your use of the Trust's IT resources.
- You must only use the user accounts that are assigned to you to access the Trust's network and IT systems. You must not use accounts of other authorised users or allow others to use your own accounts. This includes the use of smartcards to access Trust information systems.
- You must only use Trust approved systems and solutions to share information, and only share information which is appropriate, relevant and authorised.
- Staff are not to connect privately procured hardware to any of the Trust IT equipment or network without prior approval through the appropriate approval process.
- Staff should not install any software on Trust IT equipment without the prior written approval.
- Staff should not use web based portals or systems without prior written approval.
- All staff are to use complex passwords which are changed on a regular basis (maximum of 180 days).
- Failure to comply with the requirements of this policy r and may result in the rights to use Trust systems and/or resources being withdrawn, disciplinary action or prosecution under law.

TARGET AUDIENCE:

This Policy applies to all substantive and bank staff, volunteers and any other individual who has legitimate approved access to Trust devices and systems.

TRAINING

All staff are required to undertake annual Data Security and Awareness Training.

1.0 Quick look summary

Please note that this is designed to act as a quick reference guide only and is not intended to replace the need to read the full policy.

1.1 Version control and summary of changes

Version	Date	Author	Status	Comment
1.0	March 2025	Head of Data Privacy	Final	Disaggregation of content from the Information Risk and Security Policy into two policies and the addition of Artificial Intelligence information.

For Further Information Contact:
Data Protection Officer, lpt.dataprivacy@nhs.net

1.2 Key individuals involved in developing and consulting on the document

- Head of Data Privacy, LPT
- Cyber Security Manager, LHIS
- Members of the Data Privacy Group
- Policy Expert Group

1.3 Governance

Level 2 or 3 approving delivery group
Data Privacy Group

Level 1 committee to ratify policy
Finance and Performance Committee

1.4 Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

If you would like a copy of this document in any other format, please contact lpt.corporateaffairs@nhs.net

1.5 Due Regard

LPT will ensure that due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- Strategies, policies and procedures and services are free from discrimination.
- LPT complies with current equality legislation.
- Due regard is given to equality in decision making and subsequent processes.
- Opportunities for promoting equality are identified.

Please refer to due regard assessment (Appendix 4) of this policy.

1.6 Definitions that Apply to this Policy

Artificial Intelligence	Artificial intelligence (AI) is a set of technologies that enable computers to perform a variety of advanced functions, including the ability to see, understand and translate spoken and written language, analyse data, and make recommendations.
Anti-Virus	Software that provides an electronic defense mechanism mitigating the risk of a computing device being infected with or affected by malware.
Asset	Any information system, hardware, software, resource.
Breach	Any event or circumstance that led to unintended or unexpected harm, loss or damage.
Caldicott Principles	Set of Principles developed in the NHS relating to the management of patient information.
Digital Evidence	Any digitally stored evidence which may be captured and used to support a specified investigation.
Electronic Resource / Equipment	This includes computers (server, PC/workstation, laptop or any personal digital device), network assets, and any other peripheral equipment linked to the network, and also mobile phones and web enabled devices authorised for use for business which may not be linked to the network but could be used to send and receive text messages or other data.
Firewall	A firewall is security mechanism that limits access across a network connection.
Forensic/Incident Investigation readiness	The collection of digital evidence to meet the business risk assessment, and in advance of any incident occurring.
Hardware	Equipment concerning or connected to a computer is often referred to as hardware. This equipment is divided into two categories, hardware and peripherals. Hardware is the heart of any computer system enabling the processing and storing of electronic data. Hardware includes: • The base or tower unit of PC's – normally containing the processor and hard disk drive • Notebook or laptop computers • Network servers • Removable or external hard disk or zip drives • Removable or external tape drives. • Any other removable data storage devices • Smart devices (see hand held devices below)
IT Security/Cyber Security	IT security/Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programmes and data from attack, damage or unauthorised access. The overarching aim to ensure confidentiality, integrity and availability of data and IT systems.
Information Security Management System	A systematic approach to managing sensitive information relating to the business, so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

Media	Removable digital, laser, magnetic, optical or paper based information store. Examples include: - Medical records - Letters, documents, computer print-outs - USB drives - Any other make/type of equipment meeting this criterion.
Mobile Device	Any electronic device capable of creating, receiving, transmitting and storing portable data, with the ability to connect to, and exchange information with, a PC or laptop computer. This includes devices known as: - Hand held computers - Smart phones and tablets (including iOS and android devices). - Any other make/type of equipment meeting this criterion.
Monitoring	The interception of communications, monitoring systems, logging, recording, inspecting and auditing; and communication of this with nominated investigators to satisfy organisational responsibilities and obligations under the law.
Network	An infrastructure which is configured and maintained to assure performance, availability and integrity of information exchange between the computers and peripherals it connects.
Peripherals	Equipment connecting to hardware to enable input and output of electronic data; peripherals are often inter-changeable. They do not store data. Peripherals include: - Monitor - Keyboard - Mouse/trackball - Scanner - Printer - Projector
Personal Confidential Data (PCD)	The Caldicott review interpreted' **personal**' as including the **Data** Protection Act **definition of personal data**, but included **data** relating to the deceased as well as living people, and '**confidential**' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive'. The GDPR's definition of personal data is now also much broader than under the DPA. Article 4 states that "'personal data' **means** any information relating to an identified or identifiable natural person ('**data subject**')".
Registration Authority	The RA manages the registration process within the Trust, which includes the creation, distribution, and control of NHS Smartcards required for access to any NHS Care Records Service (NHS CRS), such applications include SystmOne and Electronic Staff Record.
Risk Management	The identification, assessment, and prioritization of risks. The level within the management hierarchy at which a risk is currently being managed at / has been escalated to

Senior Information Risk Owner (SIRO)	Director level manager who sits in the Board and is responsible for reporting information risk to the Board and Chief Executive.
Software	Programs loaded onto hardware may enable the user to create process and store information. Software may require a license. Software includes the operating system, Microsoft Windows and application suites such as Microsoft Office, which comprises Access, Excel, Outlook, PowerPoint and Word.

2.0 Purpose of the Policy

The aim of this policy is to establish an overarching framework, outlining the approach, methodology and responsibilities for Information security and risk that provides assurance that:

- Members of staff are aware of their responsibilities concerning security of IT resources and confidentiality of information they use and that information security is an integral part of their day-to-day business.

3.0 Summary and Key Points

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Leicestershire Partnership NHS Trust by:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other data security and protection policies.
- Creating and maintaining within the Trust a level of awareness of the need for information security as an integral part of the day to day business.

4.0 Introduction

Information is of greatest value when it is accurate, up to date and accessible from where and when it is needed; inaccessible information can quickly disrupt or devalue mission critical processes. This policy aims to preserve the principles of:

- ***Confidentiality*** – that access to data shall be confined to those with appropriate authority and protected from breaches, unauthorised disclosures of or unauthorised viewing.
- ***Integrity*** – that information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification and not allow unauthorized modification of data.
- ***Availability*** – that information shall be available, delivered to the right person, at the right time when it is needed and protected from disruption, loss and denial of service attack.

Information security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the Trust is providing a secure and trusted environment for the management of information used in delivering it business.
- Clarity over the personal responsibilities around information security expected of staff when working on Trust business.
- A strengthened position in the event of any legal action that may be taken against the Trust (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security (including addressing requirements of the Data Security and Protection Toolkit (DSPT) and forms part of the Trust Information Security Management System (ISMS) that conforms to ISO/IEC 27001).
- Assurance that information is accessible only to those authorised to have access.

- Assurance that risks are identified and appropriate controls are implemented and documented.

5.0 Duties within the Organisation

5.1 The **Trust Board** has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

5.2 The **Trust Policy Committee** is mandated on behalf of the Trust Board to adopt policies.

5.3 **Trust Board Sub-Committees** have the responsibility for agreeing policies and protocols.

5.4 **Senior Information Risk Owner** (SIRO) is accountable for:

- Information risk within the Trust and advises the Board on the effectiveness of information risk management across the Trust;
- The Trust's information risk assessment process and information management;
- Overseeing adherence to this Policy to the satisfaction of the Trust;
- Ensuring documentation and appropriate action is taken where non-compliance to this policy or a need for improvement is identified

5.5 **Caldicott Guardian** is responsible for ensuring implementation of the Caldicott Principles, National Data Guardian Standards and confidentiality and appropriate sharing of service user information throughout the Trust.

5.6 **Data Privacy Group** is responsible for ensuring that this policy is:

- In accordance with data security and protection standards;
- Implemented and understood across the Trust

5.7 **Data Protection Officer** has responsibility for ensuring that data security and protection standards are implemented effectively across the Trust. Including:

- The co-ordination, action planning and reporting of information security work and activity;
- Maintaining the Trust's Information Asset and data flow mapping registers and their regular review;
- Ensuring that investigation into all data loss is completed,

5.8 **Service Directors and Heads of Service** are Information Asset Owners and System Managers and are responsible for the protection, security and day-to-day management of designated assets/systems, including:

- Development and enforcement of system security policies and appropriate operational and administrative procedures;
- The development and maintenance of necessary business continuity and disaster recovery plans and verification of their regular testing;
- Appropriate reporting, investigation and necessary remedial/corrective action relating to incidents, security breaches and data loss associated with respective information assets.

5.9 **Human Resources Department** is responsible for ensuring:

- Information security requirements are addressed during recruitment and all contracts of employment contain appropriate confidentiality clauses;
- Information security responsibilities, duties and expectations are included within appropriate job descriptions, person specifications and HR policies and codes of conduct;
- Data security awareness training is included in the Trust's staff induction process and annual mandatory training;
- Supporting the LHIS cyber security specialists in any IT forensic investigations.

5.10 LHIS and its staff are responsible for ensuring the continuity and availability of Trust IT resources and the security and integrity of the data within its network. In addition to the other responsibilities and duties detailed in this policy,

5.11 Managers are responsible for ensuring that their permanent and temporary staff and contractors have read and understood this policy and, in addition to the other responsibilities and duties detailed in this policy, that:

- Staff are instructed in their security responsibilities, work in compliance with this policy, related processes, guidelines and safe working practices;
- Staff are appropriately trained in the use of the Trust's IT resources and systems;
- Property registers in Electronic Staff Records (ESR) are kept up to date with IT equipment that has been assigned to staff;
- Agreements are in place with suppliers and external contractors that ensure staff and subcontractors comply with appropriate policies and procedures before access to Trust systems or use of its IT resources is permitted.

5.12 All staff are personally responsible for ensuring that no breaches of IT security result from their actions and shall:

- Comply with this policy, its related processes, guidelines and safe working practices;
- Ensure that they are fully aware of the unacceptable uses of IT resources as outlined in this policy;
- Understand their responsibilities to prevent theft, protect and maintain the confidentiality and integrity of the Trust's information assets and data and security of the Trust's networks;
- Ensure operational security of information and IT equipment and systems is used;
- Receive adequate training and/or guidance in the use of any IT equipment or systems provided by the Trust in relation to their own duties and responsibilities;
- Comply with notifications that may be issued by LHIS concerning any collective or individual action that must be undertaken in response to potential or actual information security threats;
- Understand their responsibilities to accurately enter data into IT systems and take appropriate action to identify and report missing, lost and incorrect data;
- Ensure that any incident that could potentially affect the security of information is reported in a timely manner.

5.13 Other authorised users of Trust IT resources are personally responsible for ensuring that no breaches of IT security result from their actions and shall:

- Comply with this policy, its related processes, guidance and safe working practices;
- Confirm such agreement in writing, via contract, memorandum of understanding or other mutually agreed mechanism.

6.0 Policy Requirements

6.1 Use of IT Resources

The Trust's IT resources are business tools and users are obliged to use them responsibly, ethically, effectively and lawfully. Users of the Trust's IT resources shall comply with Trust policies, current safe working practices and NHS standards and best practice guidance.

Confidentiality and security clauses associated with the use of the Trust's IT systems, other IT resources and information contained within shall be appropriately included in terms and conditions of employment and addressed during recruitment.

Members of staff shall receive appropriate training in the use of the Trust's IT systems, other IT resources and personal security responsibilities before authorisation of their use is granted.

Members of staff provided with enhanced and privileged access rights (e.g. system and database administrators, Super Users, LHIS staff and similar) shall use their rights solely in the proper undertaking of their duties, and shall not deliberately access sensitive information without express and authorised permission.

With the exception of penetration and vulnerability testing that has been authorised by the SIRO, attempting to gain illegal or unauthorised access to data or systems, or seeking and exploiting weaknesses in IT systems or networks for unauthorised purposes, is a serious contravention of Trust policy and a criminal offence. It is strictly forbidden and is not tolerated under any circumstances by the Trust.

6.2 System Monitoring

In the interests of maintaining system security, complying with legal requirements, detecting and investigating unlawful activity and ensuring compliance with policies and standards is maintained, the Trust reserves the right to monitor use of its IT resources and information. This may include network access and activity, in-bound and out-bound traffic, device status and usage, session activity, password quality, e-mail usage, virus activity, web-browsing and critical event alerting.

Whilst conditional personal use of some IT resources owned by the Trust is permitted (e.g. email and internet), users should be aware that there must be no expectation of privacy. If privacy is expected, the Trust's IT resources must not be used for personal matters.

System monitoring reports will be provided as part of the cyber and information security metrics to the Data Privacy Committee for scrutiny and identification of any further actions, which may include awareness messages.

6.3 Incident Management

All users of the Trust's IT resources are personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

Potential and actual information security breaches associated with the use of the Trust's information and IT resources shall be reported and investigated in accordance with the Trust's Incident Reporting Policy and procedures.

In instances where collection, preservation and protection of digital evidence is required for legal or disciplinary matters, the Cyber Security Team will be contacted at the earliest opportunity.

6.4 Personal Use of Trust Owned Assets

The following conditions apply to use of LPT IT equipment and services for personal purposes:

- IT equipment and services are provided primarily for use for Trust purposes. Management may authorise **limited** personal use as a benefit to staff, provided this does not interfere with the performance of their duties.
- Use of IT equipment and services for private work resulting in personal commercial

gain is not permitted. (This does not apply to the provision of private healthcare services).

- The user must comply with this Policy. In particular, if taking equipment off-site, the user must comply with the rules for Agile Working policy.
- No information or software should be loaded which would compromise the use of equipment for work purposes and the Trust has disabled autorun to support the inability of staff to install unapproved software.
- No software should be loaded onto Trust equipment without express permission of the LHIS Infrastructure and Support Manager.
- Where the use of IT equipment and services for personal purposes is permitted, the user obtaining, recording or, storing information must do so in compliance with Data Protection Legislation; ensuring appropriate notification to the Information Commissioners Office where necessary. If you are unsure, please seek advice from the Data Privacy Team.

6.5 Use of Non-NHS Equipment

Use of personal devices is only permitted to facilitate security measures needed to access trust systems such as:

Accessing applications to facilitate Multi Factor Authentication (MFA) for trust systems or receiving text messages to authenticate VPN access

Personal devices are not permitted to access trust hosted Microsoft 365 systems and services including email, trust data on shared drives etc.

All employees and anyone working on behalf of the Trust, involved in the receipt, handling or communication of person identifiable information and commercial information, has a duty to adhere to this policy.

The connection of unauthorised devices on the network is prohibited where an exception is needed this must be authorised by the Data Privacy and Cyber Security Teams contact the LHIS ServiceDesk for advice.

Where the use of non-NHS owned equipment is authorised, the user is reminded of their contract of employment obligations; namely that;

- Intellectual property rights of any development is as described in the contract.
- NHS data will be removed from the device by the NHS at change of role, on leaving the organisation, or where the device is lost or stolen.
- The organisation accepts no responsibility for private information which may be lost in ensuring secure removal of NHS information.
- Non-NHS devices authorised for use for work purposes will be surrendered as required for the purposes of any audit or investigation undertaken by the Organisation.
- The user is responsible for ensuring the physical protection of the device and that the device security is maintained up to date (e.g. accepting patches), and will comply with any technical configuration requests and procedures.

Where authorised non-NHS owned devices which are smart phones and tablets, must be secured:

- Password protection will be enforced.
- Information will be passed to the device in an encrypted ‘bubble’
- Loss or theft of the device must be reported immediately to the LHIS Service Desk so that NHS information can be remotely wiped.
- When a user leaves the Trust, NHS information will be remotely wiped from the device.

Contact the LHIS Service Desk for more information.

6.6 Access Control

Access to the Trust's IT resources and systems is restricted to users who have a justified business need to access the information contained within and are authorised by the relevant information asset owner or system manager.

Identification, authentication, passwords and/or smartcards are used to ensure access to the Trust's systems, devices and information is controlled and restricted to authorised users only. For further information see the Information Security Risk Policy.

6.7 Smartcards

Please refer to the LHIS Registration Authority Procedure and the Information Security Risk Policy for more detail on the use and management of Smartcards

Smartcard Use
Smartcards must be kept at all times with the card holder and all users must sign the nationally set Terms & Conditions of Smartcard use. This reminds them of their responsibilities and obligations, including not sharing the card, leaving the card unattended, and not disclosing their passcode/PIN to others.

Cancellation of Smartcard
All leavers must retain their NHS Smartcard if there is any possibility in the future that the user will access Spine enabled systems. If leaving the NHS, they should have their access revoked accordingly and hand in their Smartcard to the RA Agent.

Lost, Stolen or Damaged Smartcards
In the event a staff member has lost, stolen or damaged their Smartcard, they should report this immediately through the LHIS ServiceDesk. The cardholder must register the incident on the incident reporting system so that it can be investigated in line with Trust policy.

Replacement of lost, stolen and damaged Smartcards incurs a cost to the NHS.

6.8 Disability Related Adjustments

Should a situation arise whereby a user has difficulty authenticating or using software or devices because of a temporary or permanent disability, reasonable alternative processes may be considered, whilst still complying with the relevant security and governance standards.

To ensure that the Trust meets it obligations under the Equality Act, authorising managers should contact the LHIS Service Desk and Data Privacy Team to enable a solution which balances the needs of the individual with the Trust's legal requirements to Data Protection legislation.

6.9 Staff Personal Drives and Mailbox

Access to staff member's personal mailbox should be requested by the mailbox owner in the first instance or by a direct line manager if the owner is absent. Please note this only applies to Trust owned mailboxes. Access cannot be granted to non-Trust owned mailboxes. All requests to grant or revoke access must come via the Self-Service Portal. All requests will be approved and managed by the LHIS Team in conjunction with the Data Privacy Team.

All data held on a user’s personal drive on the Trust network is classed as ‘live’ data and access to this by another staff member must be approved by the Data Privacy Team in conjunction with LHIS Information Security. Due to the potential of a clinical risk or patient risk, no patient data of any kind (including data relating to a patient e.g. carer info) should be held on a personal drive. All patient and any other confidential Trust related data should be kept in the Trust networked shared drives or within the clinical system, accessible only by those authorised to see the data.

Access to live data held on a staff member’s personal drive will only be granted in the following circumstances:

- The user has left the Trust and the account has been disabled via the LHIS self service portal or the appropriate form (once the account is disabled the data is classed as historical)
- For the Information Security staff to get access to data required by another staff member.
- For the Information Security staff as part of a formal investigation.

If specific data held on a staff member’s personal drive is required, a request must be submitted to the LHIS service desk either via email or the self-service portal. The Information Security staff will arrange access to the H drive and will extract the specific data and move it to a specified location.

6.10 Guidance on the Secure Use of User Accounts

- Accounts must only be accessed by the names individual to whom the account has been assigned;
- Service users must not be given access to any staff user account or devices attached to the Trust network, even under supervision;
- Sharing account login information is **prohibited** and **any** breach will be investigated by Data Privacy and Information Security personnel;
- Giving another person or persons access to your user account is **prohibited** and **any** breach will be investigated by Data Privacy and Information Security personnel;
- Login details must not be written down and stored in any location where they could be seen by an unauthorised individual;
- Passwords are changed every 180 days and must meet the following criteria:
  (a) Avoid choosing obvious passwords (such as those based on easily discoverable information).
  (b) Do not choose common passwords (use of technical means, such as using a password blocklist, is recommended).
  (c) No password reuse.
  (d) store password securely in a password protected document on a secure drive.
  (e) Smartcard passwords must memorised and not recorded anywhere.
  (f) LHIS will assess risks to ensure systems use appropriate authentication measures e.g., high-strength passwords enforced technically for all users of internet-facing authentication services
- All unattended PCs or Laptops must be locked. In this context “unattended” means out of the user’s direct line of sight;
- Admin/Super User accounts must have passwords that are changed regularly or when authorised staff leave or else be protected by an automated technical solution;
- Admin/Super User accounts should not be used for day to day business activities;
- Access rights should be granted using the principle of ‘Least Privilege’ to ensure that staff only have the rights they need to carry out their job role;
- It is the responsibility of the Information Asset Owner (IAO) of each system or Share to ensure that access rights for their system are managed appropriately and in line with the Trust policy and legal requirements;
- The authorisation and provision of access must be carried out by separate individuals

to minimise the risk of abuse.

6.11 Hardware, Software and System Security

All IT hardware, software and systems purchased must comply with legal and cyber security requirements. Portable equipment (including removable media) shall be subject to the additional measures of encryption protection and security requirements to meet national standards.

IT equipment and systems not purchased through LHIS will not be connected to the Trust's network until they have been through testing and appropriate authorisation gained for connection.

All software must be approved prior to use within the Trust. It should be noted that:

- Software includes but is not limited to systems, databases, web portals, Artificial Intelligence tools, Chat bots, wearables and apps.
- This policy refers to Apps from any source including those available from NHS approved App libraries.
- All Apps, which can range from those that provide simple information to those supporting self-management of long-term conditions, are covered by this policy.
- This policy applies equally to Apps that are recommended to patients for self-management as well as those used as part of a clinical pathway.

Any use of software meeting the definition above must be requested via LHIS through the software approval process. Requests will be reviewed in accordance with the Information Security Risk Policy prior to approval. Any use of non-approved software to process personal, sensitive or commercial data could result in disciplinary action.

6.12 Artificial Intelligence AI

The Trust recognises that AI systems, including machine learning algorithms and natural language processing, can contribute significantly to research, improving healthcare outcomes and resource allocation. However, we must ensure that AI technologies are used in a manner that aligns with legal requirements, respects patients' rights, and maintains the trust and confidence of our patients, staff, and stakeholders.

It is important to use AI appropriately and responsibly to ensure that it does not compromise personal data, business sensitive information, violate policies, or pose a risk to patient safety or our network integrity. The Trust's policy is aligned with the Gov.uk AI Playbook's 10 principles and all staff assessing the suitability of Artificial Intelligence tools through established Trust processes must ensure that these principles are considered.

This policy fully adopts the guidance of the Information Commissioner's Office and the National Cyber Security Council and as a result you must not enter sensitive information (such as personal details or company intellectual property) into unapproved software, and risk breaching Trust or patient data. All employees have a responsibility to ensure that any use of software as outlined in Section 6.11 has been reviewed against legal guidance and is safe to use.

6.13 Physical Security

- IT equipment will be sited where reasonably practicable to reduce risk from environmental threat and unauthorised access. Where equipment is kept or installed in public areas of Trust buildings, it will be positioned as far as reasonably practicable, to reduce risk of unauthorised access or casual viewing.
- Reasonable and appropriate measures shall be taken to minimise the risk of theft of the Trust's IT equipment including the secure anchoring of equipment in public areas.
- Environmental controls and monitoring systems that trigger alarms should problems occur shall be installed to protect the Trust's core and critical IT equipment.
- Ingress/Egress rights must be assigned to an individual via the use of a token such as a smartcard, fob or other physical object.
- Visitors will be provided with visitor badges for the duration of their visit and may be granted rights to non-sensitive areas at the discretion of the authorising manager and the LHIS Information Security Team
- Visitors **must not** be left unattended at any time in secure areas.
- It is the responsibility of the last person leaving a secure area to check that all the windows and doors are locked and that any alarm is activated.
- In the event of long-term absence, such as sickness or maternity leave, it is the responsibility of the authorising manager to ensure that physical access rights have been revoked pending the staff member's return.
- Access to areas housing the Trust's core and critical IT equipment will be restricted and kept secured at all times.
- Where possible core and critical IT equipment of the Trust shall be connected to secured power supplies, using uninterruptible power supplies and generator backup services to ensure that it does not fail during failure of the mains supply or switchover between mains and generated supplies.
- Uninterruptible power supplies shall be dimensioned to ensure that relevant equipment and key IT systems can be shutdown by controlled processes in the event of continuing supply failure.
- IT and communications cabling shall be protected from interception or damage (via physical fabric of the building or in conduit) and sited in accordance with relevant standards in relation to electrical and heating services.

6.14 Remote Working

Staff have the ability to access the network using corporate Wi-Fi from various locations across Leicester and Leicestershire or, via the internet using a secure remote access (VPN) solution, which is facilitated through the use of secure encrypted devices (smart phones/tablets/encrypted laptops).

6.14.1 Authorisation

Authorisation is required by a line manager that as part of your role there is a requirement to take information software, processing equipment capable of storing work related information outside of the organisation (e.g. laptops, tablets, memory cards, digital recorders, cameras, etc.).

There are team specific rules for office and off-site working patterns confirmed with the line manager.

Where equipment used for off-site (or at home) is damaged/lost, the cost of rectification will be discussed with the user and associated budget holder.

The use of IT equipment and services for private work resulting in personal commercial gain is not permitted (this provision does not apply to private healthcare services).

6.14.2 Authorisation

Portable equipment is a prime target for thieves and where it's loss includes sensitive information, the cost in public confidence is high. When using any type of mobile device or removable media, be vigilant – keep it safe! **Use approved NHS laptops, mobile devices and media only.**

Smart Devices used for work purposes will be:

- Encrypted to NHS standards
- Pin or password enforced
- Configured to prevent the storage of sensitive information in 'the cloud'
- Configured to access the secure corporate Wi-Fi
- Configured to permit remote wipe in case of loss, theft, repair, end of life
- Secured for onward use
- Disposed of securely at end of life

If your smart device is lost or requires repair or replacement contact the LHIS service desk.

6.14.3 Authorisation

All staff must follow the rules outlined below:

- Apply the rules for password or pin protection;
- Use the VPN solution for secure remote access;
- Use Ctrl Alt Delete to lock your device from view;
- Sensitive information, stored on removable media, laptop, or sent by email must be encrypted;
- If faced with sending unencrypted personal confidential data by electronic means, you must have approval. Contact the LHIS service desk for options;
- Never carry your smartcard, or access details with your mobile devices;
- Do not store confidential or sensitive work information on non-NHS or unsecured equipment or media;
- The use of non-NHS equipment or media is exceptional and must be approved by the Data Privacy Team and secured in the LHIS secure devices solution;
- Contact LHIS service desk if NHS data is stored in error on non-NHS equipment;

In transit

- Keep your portable equipment with you when travelling;
- If left in the car, it must be locked in the boot;
- Beware thieves in airports, conference venues etc.;
- Avoid work on confidential/sensitive information on trains or planes etc.;
- Guard against confidentiality breach when using a smart device;
- Store manual records securely – fasten holders and bags;
- Protect equipment from the elements and electromagnetic fields.

Working away from the Office

- In all locations, protect information from view and away from the hearing range of unauthorised people;
- For each session before printing, send a test print to confirm your printer location;
- Collect prints immediately;
- At home, log off or lock your equipment when you leave it; Elsewhere, never leave the equipment unattended;
- Store records, equipment and media safely when not in use;
- Store keys, smartcard, VPN Code receiving device separately from your laptop;
- At home use lockable storage or store out of sight, preferably upstairs

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

- Position equipment away from prying eyes, ground floor windows and sources of heat or dampness;
- Return all waste documentation, printouts and removable media to the workplace and follow the usual disposal procedures.

6.14.4 Working from Abroad

Applications to work from abroad will be considered on an individual basis
Applications to work from abroad will only be considered where there is exceptional business or clinical need.
The country you intend to work from must be deemed as low risk for Data Privacy and Cyber Security.
Applicants should complete the Application to work from abroad form which is available from lpt.dataprivacy@nhs.net
Forms will need approval from the staff member' Operational Line Manager, Data Protection Officer and Cyber Security.
Operation plans for Business Continuity and mitigation to any issues which may arise must be agreed by the business or clinical service before the application is submitted.

6.15 Backups, Software, Virus Protection

- Data should be stored in an application system or on the network for assured backup;
- Always ensure that the latest version of work related data is stored on the network as opposed to the 'C' drive of your device;
- Only authorised software may be loaded onto a device. Contact LHIS service desk for advice;
- Software supplied must not be copied;
- A virus may cause serious disruption to all systems. Do not plug in or upload any unauthorised software or device;
- Never forward a virus warning, as they are often hoaxes;
- Report suspected viruses to the Service Desk;
- Login regularly to keep your anti-virus protection up to date;
- Ensure smart device security by accepting supplier security patches and software/updates.

Further information on working in an Agile way can be found in the Trusts' Agile Working Policy.

6.16 Information Storage and Sharing

Sensitive information must:

- Only to be stored on Trust owned or controlled IT resources or authorised systems;
- Not to be intentionally placed on personal or privately owned devices and storage resources;
- Only to be sent outside the Trust with the authorisation of an appropriate Trust representative.

Staff shall only share information that is appropriate, relevant and authorised. Information that is shared electronically shall only be shared using Trust approved systems and solutions.

Information shall only be shared via email in accordance with the criteria and conditions detailed in the Trust Internet and E-Communications Policy, and Use of Electronic Communications with Service Users Policy.

Portable and removable media shall only be used to share information where secure direct transfer methods are not available, and under the following conditions:

- That it shall be in accordance with the requirements of the Trust's Remote and Mobile Working Procedures and associated IT Guidelines;
- That it is encrypted in accordance with NHS standards and guidelines;
- That, if not being transported personally by an authorised representative of the Trust, it is sent by a Trust approved courier or special (registered) delivery and confirmation of receipt must be obtained by the sender.

6.17 Covert Recording

The Trust complies with legal requirements under the Data Protection Act with regards to permitting overt and covert recordings by patients. Recordings of appointments are permitted but must be for the personal use of the patient only and must not be publicly broadcast or infringe the privacy rights of any other patients.

8.0 Training Needs

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as mandatory and role development training.

9.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
1	Members of staff will receive appropriate training	Sec 6.1	Data Security Awareness Training compliance	Data Privacy Group	Bi-monthly
2	System monitoring reports	Sec 6.2	Included in the Cyber and Information Security Reports	Data Privacy Group	Bi-monthly
3	IT incidents reported in line with Incident Reporting Policy	Sec 6.4	Number of IT reported incidents included in Cyber and Information Security Reports	Data Privacy Group	Bi-monthly
4	User account audits undertaken	Sec 6.6.2	Outputs of Audit included in Cyber and Information Security Reports	Data Privacy Group	Bi-monthly

10.0 Standards / Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
Data Security and Protection Toolkit	Submission on an annual basis

11.0 References and Bibliography

The policy was drafted with reference to the following:

- LPT Information and Security Risk Policy
- National Data Guardian Standard 2017

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

- Data Protection Act 2018
- Regulation of Investigation Powers Act 2000
- Gov.UK AI Playbook https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government
- NCSC AI Guidance https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Artificial%20intelligence&sort=date%2Bdesc
- ICO AI https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/

12.0 Fraud, Bribery and Corruption Consideration

The Trust has a zero-tolerance approach to fraud, bribery and corruption in all areas of our work and it is important that this is reflected through all policies and procedures to mitigate these risks.

Fraud relates to a dishonest representation, failure to disclose information or abuse of position in order to make a gain or cause a loss. Bribery involves the giving or receiving of gifts or money in return for improper performance. Corruption relates to dishonest or fraudulent conduct by those in power.

Any procedure incurring costs or fees or involving the procurement or provision of goods or service, may be susceptible to fraud, bribery, or corruption so provision should be made within the policy to safeguard against these.

If there is a potential that the policy being written, amended or updated controls a procedure for which there is a potential of fraud, bribery, or corruption to occur you should contact the Trusts Local Counter Fraud Specialist (LCFS) for assistance.

Appendix 1

Training Requirements

Training Needs Analysis

Training topic:	Data Security Awareness Level 1
Type of training: (see study leave policy)	x Mandatory (must be on mandatory training register) ☐ Role specific ☐ Personal development
Division(s) to which the training is applicable:	x Mental Health x Community Health Services x Enabling Services x Families Young People Children/LD/A x Hosted Services
Staff groups who require the training:	All Staff
Regularity of Update requirement:	Annually
Who is responsible for delivery of this training?	eLearning via ULearn
Have resources been identified?	Yes
Has a training plan been agreed?	Yes
Where will completion of this training be recorded?	x ULearn ☐ Other (please specify)
How is this training going to be monitored?	Monthly training reports to Managers

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

Appendix 2

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers

Respond to different needs of different sectors of the population yes/no

Work continuously to improve quality services and to minimise errors yes

Support and value its staff yes

Work together with others to ensure a seamless service for patients yes

Help keep people healthy and work to reduce health inequalities yes/no

Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance yes

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

Appendix 3

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Chris Biddle	Cyber Security Manager LHIS
Afroz Kidy	Security, RA and Assurance Manager LHIS
Sarah Ratcliffe	Head of Data Privacy, Group DPO

Circulated to the following individuals for comment

Name	Designation
Members of Data Privacy Group	
Members of IM&T Delivery Group	
Sharon Murphy	Exec Director Finance and Performance/SIRO
Gareth Jones	Group CDIO
Dr Bhanu Chadalavada	Medical Director/Caldicott Guardian
Trust Policy experts	

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.

Appendix 4

Due Regard Screening Template

Section 1	
Name of activity/proposal	Digital Acceptable Use Policy
Date Screening commenced	6th March 2025
Directorate / Service carrying out the assessment	Data Privacy Team
Name and role of person undertaking this Due Regard (Equality Analysis)	Head of Data Privacy/Group Data Protection Officer
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: The policy and procedure set out the requirements for staff to ensure that digital equipment and software is used appropriately in line with legislation and best practice guidance.	
OBJECTIVES: To support staff to meet their personal responsibilities under legislation and best practice guidance.	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Neutral
Disability	Positive – Section 6.6.10 outlines specific support to those with a disability and requiring additional resources
Gender reassignment	Neutral
Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Neutral
Race	Neutral
Religion and Belief	Neutral
Sex	Neutral
Sexual Orientation	Neutral
Other equality groups?	

Section 3	
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.	
Yes	No
High risk: Complete a full EIA starting click here to proceed to Part B	Low risk: Go to Section 4.

Section 4			
If this proposal is low risk please give evidence or justification for how you reached this decision:			
The purpose of clinical coding is to support the outputs of clinical care and ensure that through the conversion of codes to financial currency, the correct level of care can be commissioned.			
Signed by reviewer/assessor	Sarah Ratcliffe	Date	03/03/2025
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Signed by head of service	Sarah Ratcliffe	Date	03/03/2025

Appendix 5

Data Privacy Impact Assessment Screening

Data Privacy Impact Assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy.

The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.

Name of Document:	Digital Acceptable Use Policy	
Completed by:	Sarah Ratcliffe	
Job title	Head of Data Privacy/Group DPO	**Date** 03/03/2025
Screening Questions	**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	Yes	Where a new system or software is procured but there is an approval process in place to assess the risk to data privacy and security
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	No	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	Yes	Dependent on requests made but there are processes in place to assess the risk before agreement for the data flow
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes	Where a new system or software is procured but there is an approval process in place to assess the risk to data privacy and security
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	Yes	Where a new system or software is procured but there is an approval process in place to assess the risk to data privacy and security
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	Yes	Dependent on requests made but there are processes in place to assess the risk before agreement for the data flow
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	Yes	Dependent on requests made but there are processes in place to assess the risk before agreement for the data flow
8. Will the process require you to contact individuals in ways which they may find intrusive?	Yes	It is possible dependent on requests made but there are processes in place to assess the risk before agreement for the data flow

If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt-dataprivacy@leicspart.secure.nhs.uk

In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.

Data privacy approval name:	Sarah Ratcliffe, Head of Data Privacy/ Group Data Protection Officer
Date of approval	03/03/2025

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the Trust Website.