Leicestershire Partnership NHS Trust

Data Security and Protection Framework

This document sets out the framework that brings together all the requirements, standards and best practice that apply to the handling of information under the Data Security and Protection Toolkit & National Data Guardian Standards.

Key Words:	Data, Security, Guardian, Protection, Information, Governance, Framework	
Version:	5	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	24 January 2022	
Name of Author:	Head of Data Privacy/Data Protection Officer	
Name of responsible committee:	Data Privacy Committee	
Please state if there is a reason for not publishing on website:	N/A	
Date issued for publication:	January 2022	
Review date:	June 2023	
Expiry date:	1 January 2024	
Target audience:	All staff	
Type of Policy	Clinical √	Non Clinical √
Which Relevant CQC Fundamental Standards?	Good Governance	

CONTENTS

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
3.0 Draft	October 2014	Planned review and amalgamation of IG Framework, Policy and Strategy into a single document
3.0 Final	November 2014	Approval at Records & Information Governance Group
3.1 Draft	November 2016	Review in line with Trust Governance requirements
4.0 Draft	September 2018	Wholesale review to reflect the Data Security and Protection Toolkit, National Data Guardian Standards and changes in Data Protection Legislation
4.1 Draft	November 2021	Review in line with Trust Governance requirements
4.1 Final	January 2022	No Material changes

For further information contact:
Head of Data Privacy/Data Protection Officer
Email: lpt.dataprivacy@nhs.net

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.

Due Regard

An analysis on the impact on equality (Due Regard) has been included in the review of this policy. Please refer to due regard toolkit on the Equality page of the website for further advice.

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

Definitions that apply to this Policy

Legal	Established by law
Ethical	Conforming to accepted standards of conduct, in this case respecting the privacy and dignity of the patient and obtaining their consent
Asset Owners	Those responsible for the information assets used within the service
Asset Administrators	Those given delegated authority to safe guard the use and security of the information assets
Clinical Safety Management	The process of conducting clinical risk management to ensure patient safety with respect to services provided and the interrelated and interactive activities where electronic systems are used
Data Protection Impact Assessment	A process to help you identify and minimise the **data protection** risks of a project. You must do a DPIA for processing that is likely to result in a high risk to individuals. ... identify and **assess** risks to individuals
Due Regard	Having **due regard** for advancing equality involves: • Removing or minimising disadvantages suffered by people due to their protected characteristics. • Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. Encouraging people from protected groups to participate in public life • or in other activities where their participation is disproportionately low.
Information Asset	A body of knowledge that is organized and managed as a single entity. Like any other corporate **asset**, an organisation's **information assets** have financial value.
Statement of Internal Control	The mechanism for providing assurance in relation to appropriately managing and controlling resources

1.0 Purpose of the Policy

This document is required to provide assurance to individuals with the assurance that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible patient care and support employees in their work for the Trust. The Trust will establish and maintain policies and procedures to ensure that all requirements within the Data Security and Protection Toolkit (DSPT) are met.

The Data Security and Protection Requirements set out a framework bringing together all aspects of Information Governance along with the implementation of the National Data Guardian Standards. This document sets out the approach that the Trust will take to improve and assure its data security and protection activities and deliver year on year assurance through the Data Security and Protection scores.

Data Security and Protection covers all aspects of Information Governance and relates to **all** staff employed by LPT (herein referred to as 'the Trust'), private contractors, volunteers and temporary staff. The scope is:

- All information recorded, disclosed and used by the organisation
- All information systems managed by the organisation
- Any individual using information '*owned*' by the organisation
- Any individual requiring access to information '*owned*' by the organisation

2.0 Summary and Key Points

Information plays a key part in the clinical and corporate governance of Leicestershire Partnership NHS Trust (referred to from herein as "*the* Trust") and the quality in the provision of patient services, planning, performance management, assurance, and financial management relies upon accurate and available information.

The Data Security and Protection Requirements set out the steps that organisations are expected to take in demonstrating that they are implementing the ten data security standards, recommended by the National Data Guardian, Dame Fiona Caldicott and confirmed by the Government July 2017.

Performance against these standards is mandated by and reported to NHS Improvement and the Care Quality Commission (CQC) via their 'Well Led' inspection, as they form part of the standard NHS Contact.

3.0 Introduction

Information is a vital asset and resource, both in terms of the clinical management of individual patients, and the efficient management of services and its support. It plays a key part in healthcare governance, service planning and performance management. It is of paramount importance to ensure that information is managed legally, ethically and efficiently; that appropriate accountability, standards, policies

and procedures provide a robust governance framework for information management.

The Data Security and Protection Requirements are set across three leadership obligations and grouped by people, processes and technology. The strategy within this framework document has been developed taking these aspects into consideration:

- The implications of the Trusts' performance against the assertions set out in the Data Security and Protection Toolkit (DSPT)
- All relevant legislative frameworks
- Guidelines for Caldicott Guardians
- NHS Digital and NHSX priority areas for information governance
- National and local initiatives around the risk of personal data breaches (Confidentiality, Integrity and Availability).

4.0 Duties within the Organisation

Senior roles within the Trust supporting the Data Security and Protection agenda are held by the Senior Information Risk Owner (SIRO), the Caldicott Guardian, the Head of Data Privacy/ Data Protection Officer (IG Lead) and supported by the Data Privacy and Cyber Security Teams.

This framework applies to:

- All staff of the organisation, including temporary staff and contractors / sub- contractors;
- All information used by the Trust;
- All information systems managed by or used by the Trust;
- Any individual using information 'owned' by the Trust;
- Any individual requiring access to information 'owned' by the Trust

4.1 Trust Board Responsibilities

It is the role of the Trust Board to define the Trusts' policy in relation to data security and protection, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of this policy.

Information Governance within the Trust is an organisation wide responsibility providing a focus for the safe, secure and appropriate processing of information in all formats and across all levels within the organisation.

The Trust will ensure that the following roles are in place across the Trust

4.2 Senior Information Risk Owner

The SIRO is responsible for:

- Overseeing the development of an Information Security and Risk Policy, and a Plan for implementing the policy within the Data Security and Protection Framework

- Taking ownership of information risk assessment, including the review of the annual information risk statement as part of the Statement of Internal Control
- Reviewing and agreeing action in respect of identified information risks
- Ensuring the Trust's approach to information risk is effective in terms of resource, commitment and execution, and that this is communicated to all staff.
- Providing a focal point for resolution and/or discussion of information risk issues at the Board
- Ensuring that the Board is adequately briefed on information risk issues

4.3 Caldicott Guardian

The Caldicott Guardian is responsible for:

- Acting as the 'conscience' of the Trust, actively supporting work to facilitate and enable information sharing, advising on the lawful and ethical processing of information as required
- Providing a strategic role representing and championing confidentiality requirement and issues at the Board, and where appropriate, at a range of levels with the Trusts' overall governance framework
- Ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies, and standard operating procedures for staff, and oversee all arrangements, protocols and procedures where confidential information may be shared.

4.4 Data Protection Officer

The Data Protection Officer for the Trust is the Head of Data Privacy and they are responsible for managing the Trusts' information governance function - Data Privacy. This includes setting and implementing appropriate policy, procedure, code of conduct; staff training and awareness and campaigns; ensuring appropriate audits and monitoring mechanisms and supporting year on year improvements across the Trust. These activities will be reported through the Data Privacy Committee internally and externally through the Data Security and Protection Toolkit.

4.5 Cyber Security Manager

The Trust is supported in its IM&T activities by Leicestershire Health Informatics Service which includes the provision of a Cyber Security Manager. They are responsible for:

- Supporting the development and implementation of policies and procedures to protect information assets
- Supporting IM&T risk management and business continuity
- Reporting to the Data Privacy Committee on the information security status of the organisation by means of regular reports and presentation

4.6 Information Asset Owners (IAO) – Service Directors

The SIRO is supported by Clinical Directorate IAOs who are the Service Directors who are responsible for running the relevant business. Their role is to understand what information is held, what is added, and what is removed, how information is moved, who has access and why. They are responsible for:

- Addressing risks to the information assets they own and provide assurance to the SIRO on the security and use of these assets
- Ensuring that changes to the information assets are documented with a formal sign off from the Data Privacy function following the undertaking of a Data Protection Impact Assessment (DPIA)
- Being aware of what information is held and who has access to it for what purpose
- Taking steps to ensure compliance with the Trusts' Data Security and Protection Framework and associated policies

4.7 Information Asset Administrators (IAAs)

IAA's work with an information asset. They have day to day responsibility, ensure that policies and procedures are followed by staff and recognise actual or potential security incidents, and consult their IAO on incident management.

4.8 Data Privacy Committee

The Data Privacy Committee (DPC) has delegated authority and responsibility for the Data Security and Protection Agenda, and works alongside other governance groups (i.e. IM& T Committee and Clinical Effectiveness Group). The terms of reference for the group are available on request. The terms of reference are reviewed annually to ensure that there are no gaps or weaknesses in the Trust's data privacy accountability arrangements and that roles and responsibilities and responsibilities are current and in line with national guidelines and requirements.

The ultimate responsibility for Data Security and Protection in the Trust lies with the Trust Board. The Board discharges its functions through to the Finance and Performance Committee (FPC) as an assurance group to the Trust Board. The Data Privacy Committee is a Level 2 Trust Committee reporting to FPC. The DPC will through the development and routine reporting of agreed key performance indicators, identify risks, measure progress, oversee any necessary remedial action is taken and effective and provide a highlight report to FPC.

The DPC has overall responsibility for overseeing the development and implementation of this framework, which includes the Data Security and Protection policy and plan. This will be subject to periodic review and progress reports and any identified risks highlighted.

4.9 Clinical Safety Officers

The Clinical Safety Officers are responsible for ensuring that the Trust has an IT Clinical Safety Management system and it is audited and reviewed throughout the year.

4.10 All Staff

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware and they comply with information governance requirements at all times. This is a legal and professional obligation, which is also set out in the Trust

contract of employment.

5.0 Framework detail

The requirements set out in the Data Security and Protection Requirements published by the Department of Health & Social Care and NHS England are set across three leadership obligations under which data security standards are grouped: people, process and technology.

5.1 Leadership Obligation One - People

5.1.1 Senior Level Responsibility

There must be a named senior executive responsible for data and cyber security. Ideally this person will the Senior Information Risk Owner (SIRO), and where applicable a member of the Board

It is important that the role is recognised and acknowledged by the Trust and where changes are made at senior leadership level, the role is appropriately reassigned.

In order to appropriately scope and prioritise risk management efforts, it is necessary to ensure that a complete and accurate information asset register exists. As part of the identification process, it is imperative that all instances of information assets be located. In addition, information assets need to be classified in terms of sensitivity and criticality to the Trust.

It is also essential to ensure that all information assets have an identified owner. Information Asset Owners are senior individuals involved in running the relevant business. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. Identified key risks (those rated medium or high), once assessed by the SIRO, supported by the Data Privacy Committee, will be considered for inclusion on the Risk Register.

This will help promote accountability for complying with policy compliance and risk management and Data Protection Impact Assessment (DPIA) requirements throughout the Trust. The Information Risk and Data Protection Impact Assessment Policies set out clear guidance in relation to these issues.

5.1.2 Completion of the Data Security and Protection Toolkit

Organisations are expected to complete and submit an annual return on the Data Security and Protection Toolkit, demonstrating year on year improvement. The toolkit incorporates all of the ten data security standards and other aspects of information governance.

- Information Sharing

Information will be used proactively within the Trust, both for patient care and service management as determined by law, statute and best practice.

Information will be used proactively between the Trust and relevant partners to support patient care, with information sharing agreements in place setting out the formal mechanisms for sharing agreed in line with the Data Security and Protection Toolkit and the Information Commissioners Data Sharing Code of Practice.

Robust mechanisms will be used to support the ongoing capture and mapping of data flows into, across and out of the Trust.

- Openness and Confidentiality

Non-confidential information about the Trust and its services should be available to the public through a variety of media, in with the Trusts Freedom of Information Policy

The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000

The Trust will maintain and up to date Privacy Notice that provides clear information to service users and the public on information relating to their own health care, options for treatment and their individual rights.

The Trust will have clear procedures for dealing with requests from members of the public and service users.

The Trust will include details of any personal data breaches within its Annual Report

The Trust will pseudonymise data where necessary or use safe haven practices where not applicable.

- Information Quality Assurance

The Trust will establish and maintain policies and procedures for the effective management of records and information quality assurance, clinical and non-clinical, in line with legislation and codes of practice.

Information within the Trust should be of the highest quality in terms of accuracy, timeliness and relevance. Managers are expected to take ownership and seek to improve the quality of their information within their services.

The Trust will undertake or commission assessments and audits of the Trusts' data quality and records management.

Data standards will be set through a clear and consistent definition of data items, in accordance with national standards.

The Trust uses the Records Management Code of Practice (2021) as its standard for records management including the retention schedule.

- Information Security

The Trust will establish and maintain policies, procedures and standard operating procedures for the effective and secure management of its information assets and resources.

The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training

The Trust will establish and maintain personal data breach incident reporting procedures ensuring that it meets the requirements of data protection law and onward reporting to relevant authorities where appropriate, as well as ensuring robust monitoring and investigation.

Information assets and information flows will be mapped and recorded to assess and prevent unlawful processing and unnecessary use of personal data.

Registration Authority is the governance framework within which the Trust can register individuals as users to access the NHS Smartcard enabled system(s) - maintaining the confidentiality and security of patient information at all times.

The Registration Authority Service is provided under Service Level Agreement to the organisation through the Leicestershire Health Informatics Service. The team are responsible for the registration process by which users of Smartcard- enabled IT applications are authenticated (proven who they say they are beyond reasonable doubt) and authorised (enabled to have particular levels of access to particular patient data).

Having a common and rigorous approach to how users are registered and are given access to the national services, and other services, is an integral part of protecting the confidentiality and security of every patient's personal and health care details.

- Legal and Regulatory Framework

There are a number of legal and ethical obligations placed upon the Trust for:

- The use and security of personal identifiable information.
- Appropriate disclosure of information when required.
- Regulatory frameworks for the management of information via the NHS Digital Data Security and Protection Toolkit
- NHS and professional Codes of Conduct for consent to the recording and use of information.
- Operating procedures and codes of practice adopted by the NHS

The Trust will establish and maintain policies to ensure compliance with the UK GDPR/DPA 2018, Human Rights Act, Common Law Duty of Confidentiality and the Caldicott principles.

Information Rights

The Data Privacy Team has a designated Information Requests Team that deals

purely with the copious numbers of Freedom of Information Act and Subject Access Requests (under UK GDPR and the Data Protection Act). They respond to all requests received by acknowledging, finding the relevant information within the Trust, co-ordinating into a suitable response, ensure that necessary exemptions are applied whilst meeting the various legislative requirements in terms of timescales etc. This team are also responsible for providing the advice and support to the services in terms of disclosure decisions and where necessary apply other Laws (i.e. Access to Health Records for deceased patients, requests for the Police).

5.1.3 Retained General Data Protection Regulation (EU) 2016/679 UK GDPR and Data Protection Act 2018 Compliance

The Trust will establish a mechanism for monitoring work against the action plan for the implementation of the Regulation and Act. Assistance is provided through the embedding of requirements within the Data Security and Protection Toolkit.

5.1.4 Training Staff

All staff must complete appropriate annual data security and protection training.

Monitoring compliance with staff training status will be supported through the Learning and Development Team with reports from the Trusts Learning Management System (ULearn) provided to managers on a monthly basis.

The Data Privacy Committee will monitor overall compliance with the training requirements and review the training package in-year

Information Governance Training and Development is essential for the development and improvement of staff knowledge and skills relating to IG not only within the IG Team but across the Trust. The development of the IG Team is listed as a specific IG objective because of its importance.

IG training must extend beyond basic confidentiality and security awareness in order to develop and follow best practice. Staff must understand the value of information and their responsibility for it, which includes data quality, information security, records management, confidentiality, legal duty, information law and rights of access, and patient's rights in terms of a right of privacy and choice.

To ensure that different learning styles are catered for, each year a different focus in terms of delivering training is found. Training is available through face to face sessions and via ULearn. This will be available through any device (Trust owned or individual's own devices, i.e. smartphones).

Data Security awareness (Information Governance) training is a mandatory requirement for all staff and is included on induction and on annual refresher.

The organisation also utilises the following additional methods to ensure staff are trained in Data Security and Protection:

- Articles in the Trust eNewsletter
- Regular Campaigns

- Survey Monkey Questionnaires
- Policies, Procedures and Guidelines – staff have clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. IG awareness and mandatory training procedures are in place and all staff received training appropriate to their role.
- Confidentiality – staff are provided with clear guidance on keeping information secure and on respecting the confidentiality of patients/service users
- Privacy Notices – individuals are informed about the proposed use of personal information.

Audit and Spot Check Compliance

The use of the Managers Toolkit and Spot Check Compliance Checklist is aimed to:

- Help raise the awareness of Data Protection and the legal framework upon which information governance is based;
- Show the organisation's commitment to and recognition of the importance of information governance in day to day working practices;
- Identification of information risks to enable practical, pragmatic and operational specific recommendations
- Another vehicle in which to share knowledge

The focus of an audit approach is to determine whether the organisation has implemented policies and procedures to regulate the management and handling of personal information.

Communication

The Trust has a separate Data Privacy Communication Plan. The key areas of communicating are:

- Publication Scheme (FOI)
- Updating of Intranet and Internet Sites relating to Data Privacy
- Data Privacy articles/Top Tips in the eNewsletter
- Targeted communication in terms of specific projects
- Production of leaflets
- Privacy Notices
- Survey Monkey Questionnaires (or similar) as a process of testing staff understanding of a particular theme
- Campaigns and Competitions to support practical application of information governance elements

5.2 Leadership Obligation Two – Processes

5.2.1 CareCERT Advisories

The technical threats to IT services are constantly changing with new technologies and services presenting a widening profile over which a malicious attacker could operate. This 'threat landscape' is also magnified by the constant introduction of new vulnerabilities into existing and legacy technologies, especially as the Trust explores the use of technology to find efficiencies in working. This presents a challenging management environment where the balance between the provision of IM&T functionality must be tempered by the risk exposure to technical threats and malicious attack

The Trust is expected to act on CareCERT Advisories that are relevant to the organization and confirm within 48-hours that plans are in place to act on High Severity CareCERT advisories, evidencing through CareCERT Collect

The Trust will identify a primary point of contact to receive and co-ordinate the Trusts' responses to CareCERT advisories, and provide the information through CareCERT Collect

5.2.2 Continuity Planning

The Trust will ensure that there is a comprehensive business continuity plan in place to respond to data and cyber security incidents.

A proactive programme of testing the plan will be developed and implemented, with the outcomes included in reports to the Board.

5.2.3 Reporting incidents

Potential losses arising from breaches of IT and information security include physical destruction or damage to the Trust's computer systems, loss of system availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions. In addition, healthcare organisations process person identifiable data of particular sensitivity, which needs to be protected from loss or inappropriate disclosure.

The Trusts Data Protection Officer is responsible for ensuring that adequate arrangements are in place for:

- Reporting personal data breach events or incidents
- Managing information risks
- Analysing, investigating and upward reporting of events/incidents in line with the NHS Digital personal data breach reporting guidance and the Information Commissioner's Office reporting.
- IG work plans progress recommendations and learn the lessons
- Communicating IG developments and standards to staff.

Staff across the Trust are expected to report data security incidents and near misses

via the Trusts incident management system Ulysses. Any incidents that have an IM&T element are also reported to the LHIS Service Desk and escalated to CareCERT in line with reporting guidelines where appropriate.

5.2.4 Policies

All data security and protection/information governance policies are approved in principle by the Data Privacy Committee (DPC) before adoption by the Trust Policy Committee (dependent on their clinical impact).This mechanism is in accordance with the Organisation's Development of Procedural Documents Policy. All policies are made available to staff via the Intranet / Internet site and are communicated via the eNewsletter.

Existing policies are updated and new policies introduced in line with current information governance agenda. These policies provide the Trust's Staff Code of Conduct and must be read in conjunction with the Trust's Staff Handbook and Staff employment contracts.

Policies outline scope and intent and provide staff with a robust data security and protection framework whilst setting out their responsibilities as employees of the Trust. The Trust is committed to ensuring that all staff and those working with the Trust are familiar with its objectives and what is expected of staff in order to achieve these objectives. Policies and procedures are one of the key means the Trusts uses to communicate these expectations to staff. Staff are informed through local team meetings, professional meetings and the Trust eNewsletter.

5.3 Leadership Obligation Three – Technology

5.3.1 Unsupported systems

The Trust must:

- Identify unsupported systems (including software, hardware and application); and
- Have a plan in place to remove, replace or actively mitigate or manage the risk associated with unsupported systems

The Head of LHIS will be required to provide regular reports against the plan to the Finance and Performance Committee

5.3.2 On-site Assessments

The Trust must:

- Undertake on-site cyber and data security assessment where asked to do so by NHS Digital; and
- Act on the outcome of that assessment, including any recommendations, and share the outcome of the assessment with commissioners

In order to appropriately scope and prioritise risk management efforts, it is necessary to ensure that a complete and accurate information asset register exists.

As part of the identification process, it is imperative that all instances of information assets be located.

In addition, information assets need to be classified in terms of sensitivity and criticality to the Trust.

It is also essential to ensure that all information assets have an identified owner. Information Asset Owners are senior individuals involved in running the relevant business. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. Identified key risks (those rated medium or high), once assessed by the SIRO, supported by the Data Privacy Committee, will be considered for inclusion on the Risk Register.

This will help promote accountability for complying with policy compliance and risk management and Data Protection Impact Assessment (DPIA) requirements throughout the organisation. The Information Risk and Data Protection Impact Assessment Policies set out clear guidance in relation to these issues.

5.3.3 Checking Supplier Certification

The Trust is expected to ensure that any supplier of IT systems (including other health and care organisations) and the system(s) provided have the appropriate certification.

Where there are changes to systems, services or the procurement of new systems or services, the Trust will ensure that a DPIA is carried out to identify early whether there are any information or privacy risks associated with their implementation or delivery.

Contractors and Support organisations

The Trust will work to strengthen current arrangements with contractors/suppliers and support organisations to maintain the security of Trust information

The Trust will undertake a DPIA prior to entering into any agreement with an external party to process Trust data

The Trust will utilise the Data Security and Protection Toolkit for third parties where practicable to provide assurance that the third party has appropriate controls, policies and training in place.

6.0 Management of the Data Security and Protection Framework

The organisation will be responsible for implementing the Data Security and Protection Framework, which will be monitored by the Data Privacy Committee and report to FPC.

The Head of Data Privacy will work with all Directorates (clinical and non-clinical) to implement the Data Security and Protection Framework.

7.0 References

Legal and Regulatory Framework

7.1 Legal Framework

The organisation is bound by the provisions of a number of items of legislation and regulation affecting the stewardship and control of information. The main relevant legislation regulations are:

- Data Protection Act 2018
- Retained General Data Protection Regulation (EU) 2016/679 UK GDPR
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Health and Social Care Act
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations)
- Public Interest Disclosure Act 1998
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1991
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act 1974
- Re-use of Public Sector Information Regulations 2005

This list is not exhaustive

Regulatory Elements are:

- The Data Security and Protection Toolkit which requires trusts to assess their progress against set criteria
- Caldicott 2 – “To Share or Not to Share” (2013)
- National Data Guardian Standards (2017)
- Standards for Information Security Management
- NHS Confidentiality: Code of Practice (2003)
- NHS Guidance on Consent to Treatment
- Care Quality Commission Regulations
- Information Commissioners Office Code of Practice

7.2 Ethical Framework

The right to expect privacy ethically entitles a patient to the exercise of control over the content, uses of and disclosures of information about them as an individual. Respect for that privacy by staff is essential for maintaining patient trust in, and integrity of, the relationship between staff and patient.

Three official bodies provide basic principles that underpin ethical frameworks and which form part of staff working practices in implementing this policy. These are:

A. Department of Health Code on Confidentiality which includes the following important principles:

Staff should:
- Protect – look after patient's information
- Inform – ensure patients are aware of how their information is used; there should be no surprises
- Provide Choice – allow patients to decide whether their information can be disclosed and used in particular ways
- Improve practice – by always looking for better ways to protect, inform and provide choice

So that the Public/patient will:
- Understand the reasons for recording and processing information
- Give their consent for the disclosure and use of their personal information
- Gain trust in the way the NHS handles information
- Understand their rights to access information held about them

B. Caldicott principles, applying to the disclosure of patient-identifiable information are:

- Justify the purpose for using confidential information
- Use confidential information only when it is necessary
- Use the minimum necessary
- Access to personal data should be on a strict need to know basis
- Everyone with access to confidential information should be aware of their responsibilities
- Comply with the law
- The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Inform patients and service users about how their confidential information is used

C. The Office of the Information Commissioner has specific responsibilities under the UK GDPR and Data Protection Act 2018. This Act provides a framework to ensure that personal information is handled properly.

The Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Additionally, all staff should be familiar with their own professional codes relating to ethical aspects of information governance (i.e. respect for patient privacy and dignity).

8.0 Data Security and Protection Plan

This Plan sets out the approach taken within the Trust to provide a robust Data Security and Protection Framework for the current and future management of information.

Data Security and Protection encompasses the following initiatives or work areas:

- Information Governance Management
- Leadership Obligation One – People
- Leadership Obligation Two – Processes
- Leadership Obligation Three - Technology

Others may be included as the scope of the agenda widens

8.1 Purpose of the Plan

The purpose of this plan is to set out the approach that Leicestershire Partnership NHS Trust (LPT), will take to provide a robust Data Security and Protection Framework for the future management of information assets.

This strategy has been developed taking into consideration:

- LPT self assessment against national Information Governance requirements including the Data Security and Protection Toolkit, NHS Operating Framework and CQC Registration.
- Relevant legislative framework
- Guidelines for Caldicott Guardians
- NHS Digital priority areas for Information Governance including compliance with the NHS Care Record Guarantee
- The organisations Corporate Risk Register highlighting the need for improved Information Governance assurance
- Internal and external audit expectations and recommendations

There are two key components underpinning this strategy:

- A focus on the risks associated with information assets;
- An annual action plan arising from a baseline assessment against requirements set out in the Data Security and Protection Toolkit.

8.2 Responsibilities for delivering this plan

- The Board is responsible for ensuring that sufficient resources are made available to support the requirements of this plan.
- The Finance and Performance Committee on behalf of the Board will be responsible for the overseeing of the delivery, evaluation and monitoring of outcomes of this plan.

- The Data Privacy Committee will be responsible for implementing the plan.
- The Data Privacy Team will be responsible for the operational delivery and monitoring the implementation of the strategy and subsequent action plans

8.3 Wider Implications of Data Security and Protection

This plan cannot be seen in isolation as information plays a key part in Corporate Governance; Strategic Risk; Clinical Governance; service planning and redesign; service delivery and performance management. The continual implementation of this strategy will undoubtedly reduce the level of risk.

The focus on the risks associated with information assets will be captured on the Information Asset Register. This will include the identification of Information Assets and Information Asset Owners, information governance risk assessments, control measures, and where necessary the completion of Data Protection Impact Assessments and the agreement of Information Sharing Protocols and Agreements.

Inbound and outbound data flows will be ‘mapped’ assessed and revised to mitigate risks of breaches to confidentiality and data security.

8.4 Associated Data Security and Protection Policies/Strategies

- Information Security and Risk Policy
- Freedom of Information Policy
- Information Lifecycle and Records Management Policy
- Data Protection and Information Sharing Policy
- Individuals Information Rights Policy

This is not an exhaustive list and map of IG related policies and procedures is available on the Trust website

8.5 Data Security and Protection Action Plan

The Trust Data Security and Protection work plan is the framework developed to establish the overall direction of data privacy and the baseline principles and objectives for a robust information handling culture that permeates throughout the organisation. It sets out a programme of development to achieve and inform everyone’s approach as to how they perform their daily tasks around information and its security regardless of seniority. An Action Plan aligned to Data Security and Protection supports the delivery of the Toolkit standards.

Fundamental to the success of delivering the Data Security and Protection Plan is developing a data privacy culture within the organisation. This includes the establishment of relevant sub groups as part of the wider governance agenda. Awareness and training needs to be provided to all staff that utilise information in their day-to-day work to promote this culture. In order to achieve this, a mandatory training plan has been developed.

9.0 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 training.

The course directory on e-source will identify who the training applies to, delivery method, the update frequency, learning outcomes and a list of available dates to access the training.

A record of the event will be recorded on ULearn

The governance group responsible for monitoring the training is the Data Privacy Committee

10.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
10	There must be a named senior executive responsible for data and cyber security	Section 5.1.1	Noted at Board Meeting	Finance and Performance Committee	Changes within the Executive Team
10	The Trust must complete its Data Security and Protection Toolkit return	Section 5.1.2	Action plan	Data Privacy Committee	Quartlery
13	The Trust will demonstrate it compliance with the UK GDPR and DPA 2018	Section 5.1.3	Action Plan	Data Privacy Committee	Quarterly
13	All staff must undertake annual data security awareness training	Section 5.1.4	Training status reports	Data Privacy Committee	Bi-monthly
15	The Trust will respond to CareCERT advisories	Section 5.2.1	Status Reports	Data Privacy Committee	Bi-monthly
16	Staff are expected to report data breaches	Section 5.2.3	Personal data breach report	Data Privacy Committee	Quarterly
16	The Trust is expected to identify any unsupported systems or software	Section 5.3.1	IM&T Report	Finance and Performance Committee	Quarterly

11.0 Links to Standards/Performance Indicators

This policy links directly to work required under the Annual Data Security and Protection Toolkit return.

11.1 Standards/Key Performance Indicators

Target/Standards	Key Performance Indicator
Meet all mandatory requirements in each of the Data Security and Protection assertions	Overall Data Security and Protection Assessment

Appendix 1

Policy Training Requirements

The purpose of this template is to provide assurance that any training implications have been considered

Training Required	YES ✓	NO
Training topic:	Data Security Awareness (Information Governance) Training	
Type of training:	✓Mandatory (must be on mandatory training register) ✓ Role specific ☐ Personal development	
Directorate(s) to which the training is applicable:	✓ Adult Learning Disability Services ✓ Adult Mental Health Services ✓ Community Health Services ✓ Enabling Services ✓ Families Young People Children ✓ Hosted Services	
Staff groups who require the training:	All staff groups	
Regularity of Update requirement:	Annually	
Who is responsible for delivery of this training?	eLearning through Learning and Development	
Have resources been identified?	See Learning and Development Prospectus	
Has a training plan been agreed?	See Learning and Development Prospectus	
Where will completion of this training be recorded?	✓ Trust learning management system ☐ Other (please specify)	
How is this training going to be monitored?	Monthly reports to managers and Specialist subject leads	

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	✓
Work continuously to improve quality services and to minimise errors	✓
Support and value its staff	✓
Work together with others to ensure a seamless service for patients	✓
Help keep people healthy and work to reduce health inequalities	☐
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	✓

Appendix 3

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Sam Kirkland	Head of Data Privacy

Circulated to the following individuals for comment

Name	Designation
Sharon Murphy	Director of Finance and Performance/SIRO
Members of Data Privacy Committee	

Appendix 4

Due Regard Screening

Section 1	
Name of activity/proposal	Data Security and Protection Framework (Including policy & Plan)
Date Screening commenced	
Directorate / Service carrying out the assessment	Enabling/ Information Governance
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland, Head of Data Privacy
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: To meet the Trust's obligations under national Data Security and Protection Framework	
OBJECTIVES: To ensure that information is handled safely, securely and its integrity maintained at all steps of processing	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Positive – information rights are the same for all individuals
Disability	Positive – information rights are the same for all individuals
Gender reassignment	Positive – information rights are the same for all individuals
Marriage & Civil Partnership	Positive – information rights are the same for all individuals
Pregnancy & Maternity	Positive – information rights are the same for all individuals
Race	Positive – information rights are the same for all individuals
Religion and Belief	Positive – information rights are the same for all individuals
Sex	Positive – information rights are the same for all individuals
Sexual Orientation	Positive – information rights are the same for all individuals
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 <u>tick</u> 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:
All individuals have the same rights in law to have their information managed and stored in a

safe and secure way, whilst maintaining its integrity			
Signed by reviewer/assessor	Sam Kirkland	**Date**	09/11/2021
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed	Sam Kirkland	**Date**	31/12/2021

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:	Data Security and Protection Framework	
Completed by:	Sam Kirkland	
Job title	Head of Data Privacy	**Date**

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.	No	
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?	No	
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?	No	
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.	No	
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?	No	
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.	No	
8. Will the process require you to contact individuals in ways which they may find intrusive?	No	

If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt.dataprivacy@nhs.net
In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.

Data Privacy approval name:	
Date of approval	**31/12/2021**

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