

Data Protection Impact Assessment Policy and Procedure

Projects and/or processes that involve using or sharing personal information or intrusive technologies give rise to privacy issues and concerns. Article 35 of the General Data Protection Regulation (EU) 2016/679 as enshrined in UK-GDPR which requires data protection impact assessments to be carried out in these circumstances. This policy and Toolkit provides the framework to ensure the Trust complies with the law.

Key Words:	Impact assessment data	
Version:	3	
Adopted by:	Trust Policy Committee	
Date this version was Adopted:		
Name of Author:	Head of Data Privacy	
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:	April 2023	
Review date:	October 2025	
Expiry date:	April 2026	
Target audience:	All Staff	
Type of Policy	Clinical ✓	Non Clinical ✓
Which Relevant CQC Fundamental Standards?	Regulation 17: Good Governance	

Contents

1.0	Equality Statement	3
2.0	Due Regard	3
3.0	Definitions	4
4.0	Purpose	5
5.0	Summary	6
6.0	Introduction	6
7.0	Data Protection Impact Assessment Process Flow	7
8.0	Duties of the organisation	9
8.1	Trust Board	9
8.2	Chief Executive	9
8.3	Senior Information Risk Owner (ICO)	10
8.4	Data Privacy Lead	10
8.5	Data Privacy Team	10
8.6	Information Asset Owners (IAO)	10
8.7	Information Asset Administrators – LHIS Application Support Team and identified Directorate Leads	10
8.8	Information Security	11
8.9	All Trust Employees	11
9.0	Data Protection Impact Assessment	11
9.1	Data Protection Impact Assessment Initial Assessment	11
9.2	Full Data Protection Impact Assessment	11
9.3	Review of the Data Protection Impact Assessment	12
9.4	Identification of high risks to the Information Commissioners Office	17
9.5	High Risk Processing Outcomes	17
10.0	Training	17
11.0	Links to Standards/Performance Indicators	17
12.0	Monitoring Compliance with this Procedure	18
13.0	References and Bibliography	24

Appendices

Appendix 1 Training Requirements – Mandatory if any are identified

Appendix 2 The NHS Constitution.

Appendix 3 Stakeholders and Constitution

- Appendix 4 Due Regard Screening Template**
- Appendix 5 Privacy Impact Assessment Screening Template**
- Appendix 6 Referencing Guidance**
- Appendix 7 CQC fundamental Standards**

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
1.0	March 2014	First draft for consultation
1.1	May 2014	Final draft following consultation, for approval
1.1	June 2014	Final to Policy Group
1.2	September 2016	Draft for review consultation
1.2	November 2016	Draft for sign off by Policy Support Team
2.0	November 2019	Complete review to reflect changes in Data Protection Law
3.0	September 2022	Review and update of content

For further information contact:
Data Privacy Team lpt.dataprivacy@nhs.net

1.0 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.

2.0 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

3.0 Definitions that apply to this Policy

Anonymisation	The process of turning data into a form which does not identify individuals and where re-identification is not likely to take place
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Protection Impact Assessment	A risk technique required under Data Protection Law to enable organisations to address privacy concerns and ensure appropriate safeguards are addressed and built in as projects or plans to develop existing information assets.
Due Regard	Having due regard for advancing equality involves: <ul style="list-style-type: none"> • 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 organised and managed as a single entity. Like any other corporate asset, an organisation's information assets have financial value. The value of the asset increases in direct relationship to the number of people who are able to make use of the information. An asset extends beyond physical goods or hardware, and includes software, information, people and reputation.
Innovative Technologies	New developments in technological knowledge in the world at large Examples of processing using innovative technology include: <ul style="list-style-type: none"> (a) artificial intelligence, machine learning and deep learning; (b) connected and autonomous vehicles; (c) intelligent transport systems; (d) smart technologies (including wearables); (e) market research involving neuro-measurement (e.g. emotional response analysis and brain activity); (d) some 'internet of things' applications, depending on the specific circumstances of the processing.
Personal data	Defined under Article 4(1) of GDPR: Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or

	social identity of that natural person
Privacy	In its broadest sense, it is about the right of an individual to be 'left alone'. The Oxford Dictionary Definition is: 'A state in which one is not observed or disturbed by other people'
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Processing	Defined under Article 4(2) of GDPR as: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Projects / plans to develop	Data Protection impact assessments are required when new projects occur (for example introduction of a new electronic patient record) or where plans are proposed to develop an existing information asset. These can be both paper and electronic.
Pseudonymisation/ Pseudonymised data	Pseudonyms systematically allow two or more identifiable data items to be linked without the need to identify the individual. Pseudonymisation enables the NHS and its partner agencies to undertake secondary use of service user data in a legal, safe and secure manner
Special Category Data	Defined under GDPR Article 9(1) as data consisting of information as to: <ul style="list-style-type: none"> (a) the racial or ethnic origin of the data subject (b) their political opinions (c) religious or philosophical beliefs (d) whether they are member of a trade union (e) genetic data (for the purpose of identifying a unique individual) (f) biometric data (for the purpose of identifying a unique individual) (g) data concerning health (h) data concerning a natural person's sexual life or sexual orientation

4.0 Purpose of the Policy

The aim of a Data Protection Impact Assessment is to ensure that an organisation takes a privacy by design approach when designing projects, processes, products or systems and that privacy risks can be minimised.

There is a legal requirement under the General Data Protection Regulation (GDPR) (EU) 2016/679 Article 35 as enshrined in UK-GDPR for Data Privacy Impact Assessments to be conducted where the processing of personal data is likely to result in a high risk to the privacy rights and freedoms of individuals

This Policy and Toolkit supports the Trusts obligations in meeting this requirement and helps to demonstrate that it has integrated core privacy considerations into existing project management and risk management methodologies and policies.

This Policy and Toolkit also intends to provide appropriate and relevant guidance in regard to the completion of a Data Protection Impact Assessment to address privacy risks and concerns.

5.0. Summary and scope of the Policy

- Where there are any changes are made to systems or processes, new products or systems procured, or information shared or used in a different way and the processing of personal data is impacted, there is a legal requirement to consider privacy by design and default and undertake a Data Protection Impact Assessment.
- The process must be embedded into project management processes to ensure that privacy is at the heart of the way that data is handled and managed
- Data Protection Impact Assessment is a risk management process for assessing the risk to information processes
- Where there are high risk processing activities that cannot be mitigated, the Data Protection Impact Assessment will require scrutiny by the Information Commissioners Office prior to any processing taking place

6.0. Introduction

The introduction of the GDPR in May 2018 introduced a principle of ‘accountability’ requiring organisations to demonstrate compliance. One key obligation is in routinely conducting and reviewing Data Protection Impact Assessments where the processing is likely to pose a high risk to individuals’ rights and freedoms.

This is also one way that the Trust can ensure that privacy by design and default is embedded into its project and risk management approach when designing new ways of working, processes, systems and the purchasing of products and systems. This can lead to benefits which include:

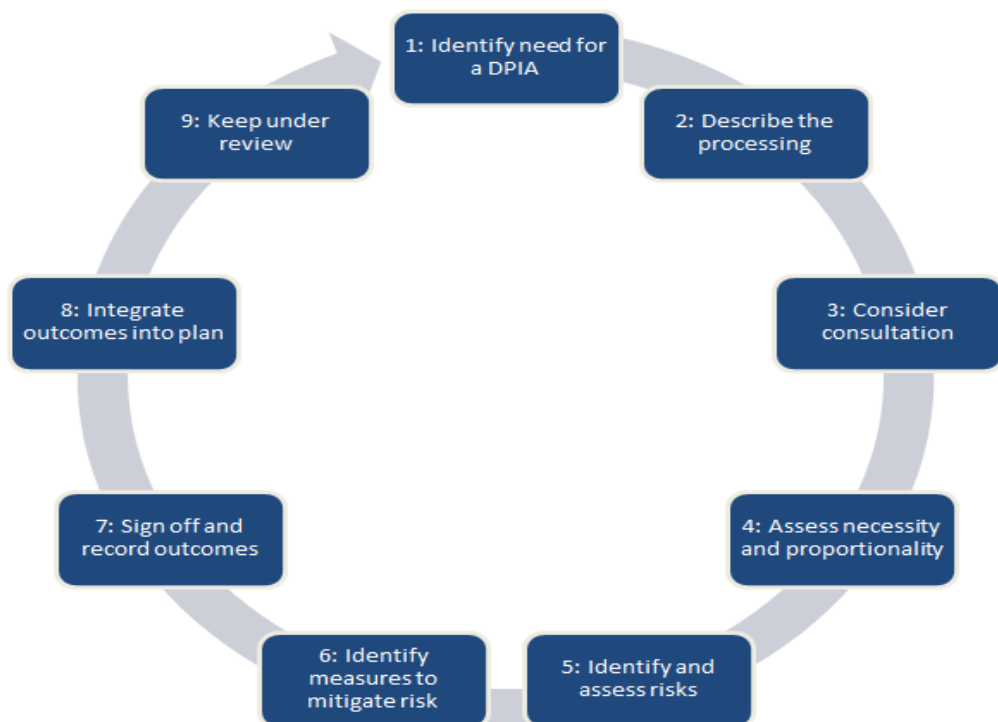
- potential problems are identified at an early stage, when addressing them will often be simpler and less costly;
- Increased awareness of privacy and data protection across the Trust;
- The Trust and other organisations within the ‘System’ and beyond, that we work with are more likely to meet the legal obligations and less likely to breach legislation;
- Actions are less likely to be privacy intrusive and have a negative impact on individuals, be they service users, family, friends or staff.

Typical examples of when a Data Protection Impact Assessment (DPIA) will be required

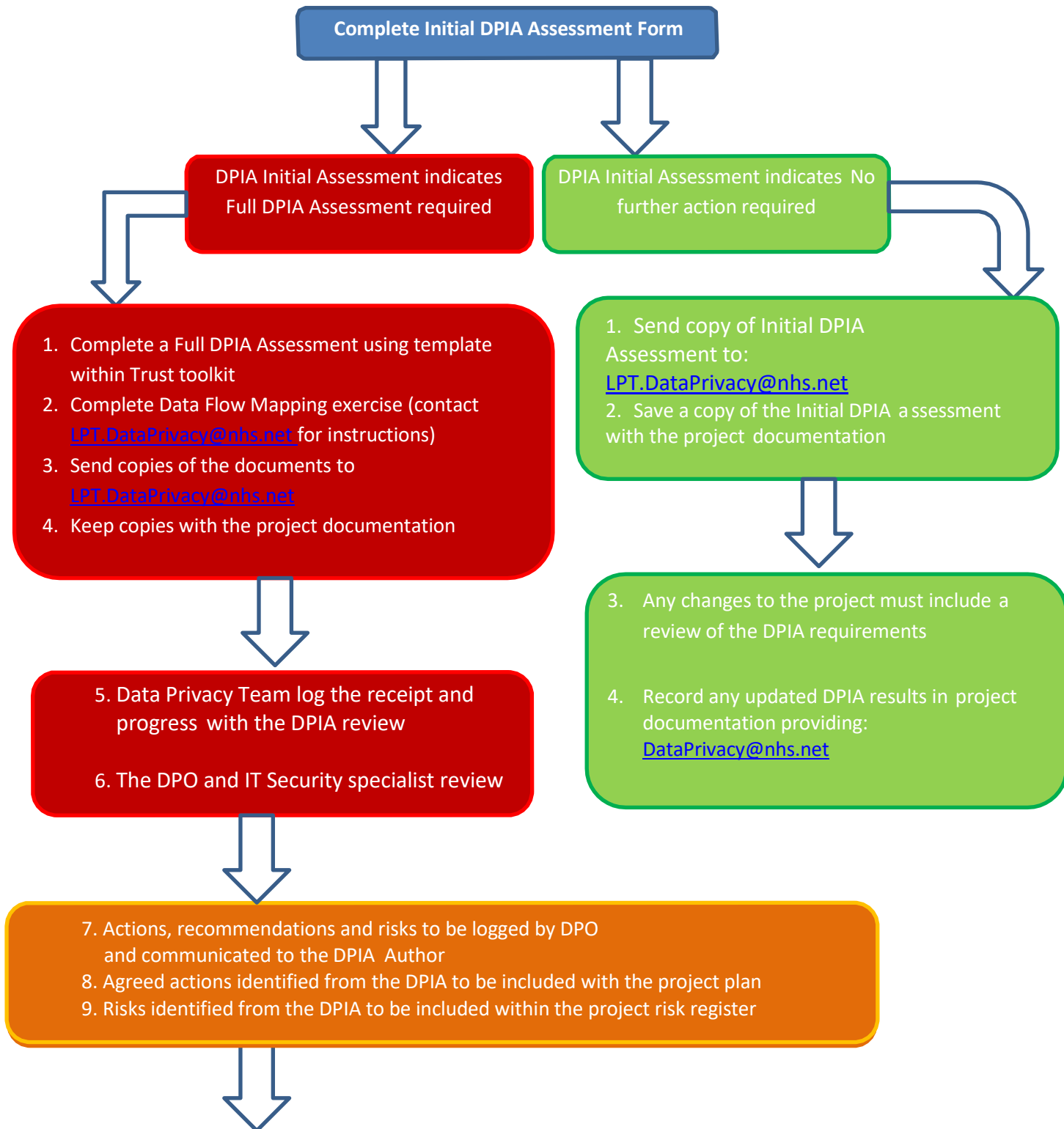
are:

- Introduction of a new paper or electronic information system to collect and hold personal or special category (sensitive) data
- Introduction of new services or changes to existing processes, which may impact on an existing information system
- Update or revision of a key system that might alter the way in which the Trust uses, monitors and reports personal and sensitive information
- Replacement of an existing information system with new software
- Plans to outsource business processes involving the storing and processing of personal sensitive data
- Plans to transfer services from one provider to another that will include the transfer of information assets
- Any change to, or introduction of, new information sharing agreements

7.0 DPIA Process Flow



DPIA Assessment Flowchart



10. Where the project involves external organisations an Information Sharing Agreement (ISA) must be produced and approved (if there is currently none in place)
11. Caldicott Guardian review and authorisation for ISA



12. Project to consider Public/Patient engagement in relation to any changes identified regarding the use of data



14. Resulting DPIA will –

- Identify all current and proposed data flows and all current and intended data sharing with other agencies
- Identify external agencies who will be involved
- Identify IT systems or technology and processes involved
- Ensure that any new assets to be created or new information systems are recorded on the Trusts' Information Asset Register

15. The DPIA is not a static document and must be updated at regular intervals throughout the project

8.0 Duties within the Organisation

The adherence to the DPIA Policy and Toolkit is essential for assuring aspects of the privacy agenda are maintained and supported by

8.1 Trust Board

In his communications with NHS Trusts Chief Executives, the NHS Chief Executive has made it clear that ultimate responsibility for IG in the NHS rests with the Board of each organisation.

8.2 Chief Executive

The Trust's Accountable Officer is the Chief Executive who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risk is handled in a similar manner to other risks such as financial, legal and reputational risks.

Reference to the management of information risks and associated information governance practice is now required in the Statement of Internal Control which the Accounting Officer is required to sign annually.

8.3 SIRO (Senior Information Risk Owner)

The SIRO is the Director of Finance. The role:

- Is accountable;
- Fosters a culture for protecting and using data;
- Provides a focal point for managing information risk and incidents
- Is concerned with the management of all information assets.

The SIRO is an executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

8.4 Data Protection Officer & Data Privacy Team

The Data Protection Officer (DPO) is the Head of Data Privacy. They are responsible for ensuring the organisation meets its statutory and corporate responsibilities.

The DPO is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of data privacy.

The Data Privacy Team are responsible for logging and oversight of all DPIA's.

8.5 Clinical Safety Officers

The Clinical Safety Officer (CSO) is a trained, accredited clinician responsible for the identification, assessment and mitigation of direct and indirect clinical hazards to patients produced by the standard use of technology in patient care. The CSO reports directly to the Chief Clinical Information Officer (CCIO) for all matters relating to clinical risk and safety management.

The CSO brings clinical oversight, experience and assurance in providing advice to the development of clinically safe standards. In doing so the CSO assists in the interpretation of best practice, the consideration of clinical risk and the evaluation of mitigating actions.

8.6 Information Asset Owners (IAO) – Directorate Directors

The SIRO is supported by IAO's who are involved in 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. As a result they are

able to understand and address risks to information assets they “own” and to provide assurance to the SIRO on the security and use of the assets.

8.7 Information Asset Administrators (IAA) – LHM Application Support Team and identified Directorate Leads

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

8.8 Information Security

The LHM Cyber and Information Security function is responsible for the provision and management of a high quality, customer focused, Information Technology Security Advisory Service using expertise to manage security issues, identifying best practice and making recommendations for local implementation.

8.9 All Trust Employees

All Trust employees and anyone else working for the organisation (e.g. Agency staff, honorary contracts, management consultants etc) who use and has access to Trust information and/or IT Systems must understand their personal responsibilities for data privacy and compliance with UK Law. All staff must comply with Trust policies and are responsible for Information Security and the correct use of Information Asset.

9.0 Data Protection Impact Assessment

A Data Protection Impact Assessment must be completed every time there is a new or changed project, process, product or system introduced involving personal and/or sensitive information or intrusive technologies which give rise to privacy issues and concerns.

9.1 Data Protection Impact Assessment Initial Assessment

Prior to the start of a new or changes project, the designated responsible officer must complete a DPIA Initial Assessment questionnaire, which allows for the initial risk assessment of the project to take place prior to the implementation of the project and before any costs are incurred.

The DPIA Initial Assessment has a number of questions with Yes/No answers. If **any** of the answers are recorded as 'yes' on this document, a full DPIA is required. The Forms can be located on the Trust intranet Data Privacy pages.

Where a DPIA is identified as **not** being required, this must be documented in the business case and/or project documentation of the new or changed system/process.

A copy of the DPIA Initial Assessment must be sent via email to the Data Privacy Team (LPT.DataPrivacy@nhs.net) for logging. A further copy must be retained with the project documentation.

9.2 Full Data Protection Impact Assessment

If a full DPIA is required a Data Protection Impact Assessment Form must be completed and sent via email to the Data Privacy Team (LPT-.DataPrivacy@nhs.net) to be logged and reviewed. Forms can be found on the Staffnet Data Privacy page at the following link:

<https://staffnet.leicspart.nhs.uk/support-services/data-privacy/data-privacy-contacts-and-policies/>

The completed DPIA Form must reflect:

- The purpose of the data processing activity
- Who the Controllers (sole or joint) and Processors (the DPIA form has the guidance)
- The legal basis for the sharing of information i.e. consent or other legal basis
- The information types (data fields and classes)
- How the data will flow and where it will be held
- What the risks are to its security (both in transit and at rest)
- The information lifecycle i.e. what triggers the creation of new data and how long it is proposed to store the data

This stage of the assessment requires as much information as possible. Within the template there is the ability to link other documents which may support the project or considerations made.

Questions answered throughout the DPIA process will help identify where there is a risk that the project will fail to comply with the relevant data protection legislation, and other associated legislation such as the Human Rights Act.

9.3 Review of the Data Protection Impact Assessment

The Data Protection Officer (DPO) and the IT Security specialist(s) will review the completed DPIA form to establish the level of privacy required and any risks identified.

The Data Privacy Team will maintain a log of all completed DPIAs

The DPO and Information Security specialists will complete the 'report' section of the DPIA form and feedback the result to the author.

Copies of the DPIAs will be used as evidence for the Data Security and Protection Toolkit.

The DPIA documentation may be required as evidence during investigations of personal data breaches/incidents.

The recommendations following the review will require the capturing of any risks on the project risk register.

All new Information Assets identified as part of the process will be reviewed and logged on the Trusts' Information Asset Register.

The Trust is required to maintain a record of all its processing activities, and as part of the DPIA process data flow mapping must be undertaken in order that the record of processing activity (ROPA) can be updated and reflected in the Trusts' Privacy Notice.

The outputs of the DPIA will be reported through to the Data Privacy Committee as part of the data privacy assurance programme.

The following list are processing activities for which the ICO requires a DPIA to be completed as they are likely to result in 'high risk'. This list is not definitive or exhaustive and is taken from ICO guidance:

Type of processing operation(s) requiring a DPIA	Description	Non-exhaustive examples of existing areas of application
Innovative technology	<p>Processing involving the use of new technologies, or the novel application of existing technologies (including AI).</p> <p>A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from WP248rev01.</p>	<p>Artificial intelligence, machine learning and deep learning</p> <p>Connected and autonomous vehicles</p> <p>Intelligent transport systems</p> <p>Smart technologies (including wearables)</p> <p>Market research involving neuro-measurement (i.e. emotional response analysis and brain activity)</p> <p>Some IoT applications, depending on the specific circumstances of the processing</p>

Denial of service	Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special-category data.	Credit checks Mortgage or insurance applications Other pre-check processes related to contracts (i.e. smartphones)
Large-scale profiling	Any profiling of individuals on a large scale	Data processed by Smart Meters or IoT applications Hardware/software offering fitness/lifestyle monitoring Social-media networks Application of AI to existing process
Biometric data	Any processing of biometric	Facial recognition systems

	<p>data for the purpose of uniquely identifying an individual.</p> <p>A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01</p>	<p>Workplace access systems/identity verification</p> <p>Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)</p>
--	--	--

<p>Genetic data</p>	<p>Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.</p> <p>A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01</p>	<p>Medical diagnosis DNA testing Medical research</p>
<p>Data matching</p>	<p>Combining, comparing or matching personal data obtained from multiple sources</p>	<p>Fraud prevention Direct marketing Monitoring personal use/uptake of statutory services or benefits Federated identity assurance services</p>
<p>Invisible processing</p>	<p>Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort (as provided by Article 14.5(b).</p>	<p>List brokering Direct marketing Online tracking by third parties Online advertising Data aggregation/data aggregation platforms Re-use of publicly available data</p>
	<p>A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14.5(b) when combined with any other criterion from WP248rev01</p>	

<p>Tracking</p>	<p>Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.</p> <p>A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01</p>	<p>Social networks, software applications</p> <p>Hardware/software offering fitness/lifestyle/health monitoring</p> <p>IoT devices, applications and platforms</p> <p>Online advertising</p> <p>Web and cross-device tracking</p> <p>Data aggregation / data aggregation platforms</p> <p>Eye tracking</p> <p>Data processing at the workplace</p> <p>Data processing in the context of home and remote working</p> <p>Processing location data of employees</p> <p>Loyalty schemes</p> <p>Tracing services (tele-matching, tele-appending)</p> <p>Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing</p>
<p>Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services</p>	<p>The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.</p>	<p>Connected toys</p> <p>Social networks</p>
<p>Risk of physical harm</p>	<p>Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.</p>	<p>Whistleblowing/complaint procedures</p> <p>Social care records</p>

9.4 Identification of high risks to the Information Commissioners Office

If the DPIA process identifies a high risk that cannot be reduced or mitigated, the project cannot proceed without consultation with the Information Commissioners Office (ICO).

The focus is on the 'residual risk' after taking mitigating measures. Where the DPIA process identified a high risk but mitigating measures have been taken and it is no longer considered high, there is no requirement to consult with the ICO.

Where it is identified that consultation with the ICO is required, a copy of the completed DPIA should be sent by the Data Privacy Team who will liaise with the Information Commissioners Office.

Where the ICO provides advice under the prior consultation process, they will respond within 8 weeks of receipt of the DPIA. In complex cases this can be extended to a maximum of 14 weeks, however the Trust will be advised if this is the case.

9.5 High Risk Processing Outcomes

The ICO may advise that based on the DPIA, that the risks have been sufficiently identified and mitigated and that the processing may proceed. Any written response could be limited to advice on how the Trust can further mitigate identified risks before proceeding with the processing.

If there are more significant concerns, the ICO may impose a limitation or ban on the intended processing.

The Data Privacy Team will keep the requestor updated on the outcomes of the ICO decision and provide advice and guidance.

10.0 Training

All staff are required to complete Data Security Awareness Training Level 1 annually.

11.0 Links to Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
GDPR Article 35	100% new projects, changes in systems/services and changes in data processing have DPIA completed
Compliance with Data Security and Protection Toolkit/National Data Guardian Standard 1	The use of personal information is subject to data protection by design and by default

12.0. Monitoring Compliance with this Procedure

The table below outlines the Trusts' monitoring arrangements for this policy/document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
12	A DPIA Initial Assessment questionnaire is required prior to the start of a new or changes project	Section 9.1	Project documentation and DPIA log	Data Privacy Committee	Escalation to Data Privacy Committee as required
12	A Full DPIA Assessment is completed where any 'yes' answers appear on the initial questionnaire	Section 9.2	Project documentation and DPIA log	Data Privacy Committee	Escalation to Data Privacy Committee as required

Training Requirements

Training Needs Analysis

Training topic:	
Type of training: (see study leave policy)	<input type="checkbox"/> Mandatory (must be on mandatory training register) <input type="checkbox"/> Role specific <input type="checkbox"/> Personal development
Division(s) to which the training is applicable:	<input type="checkbox"/> Adult Mental Health & Learning Disability Services <input type="checkbox"/> Community Health Services <input type="checkbox"/> Enabling Services <input type="checkbox"/> Families Young People Children <input type="checkbox"/> Hosted Services
Staff groups who require the training:	<i>Please specify...</i>
Regularity of Update requirement:	
Who is responsible for delivery of this training?	
Have resources been identified?	
Has a training plan been agreed?	
Where will completion of this training be recorded?	<input type="checkbox"/> ULearn <input type="checkbox"/> Other (please specify)
How is this training going to be monitored?	

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	√

Stakeholders and Consultation

Key individuals involved in developing the document

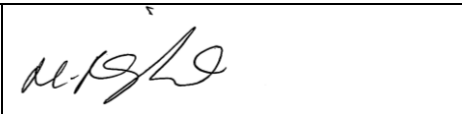
Name	Designation
Chris Biddle	Cyber Security Manager
Hannah Plowright	Data Privacy and Information Governance Manager/Deputy Data Protection Officer
Sarah Ratcliffe	Data Protection Officer

Circulated to the following individuals for comment

Name	Designation
Members of Data Privacy Committee	
Members of IM&T Committee	
Members of IM&T Delivery Group	
CHS Directorate Business Team	
FYPC Directorate Business Team	
AMH/LD Directorate Business Team	
Business Development Team	
Russell Hadfield	Clinical Category Manager
Sarah Holliehead	Head of Procurement

Due Regard Screening Template

Section 1			
Name of activity/proposal		Data Protection Impact Assessment	
Date Screening commenced		21/10/2022	
Directorate / Service carrying out the assessment		Enabling/Data Privacy	
Name and role of person undertaking this Due Regard (Equality Analysis)		Hannah Plowright Data Privacy and Information Governance Manager/Deputy Data Protection Officer	
Give an overview of the aims, objectives and purpose of the proposal:			
AIMS: To ensure that any procurement of new or changes to systems, process, information handling, and exploitation of information technology protects the privacy rights of all individuals who will have contact with the Trust.			
OBJECTIVES: To ensure that information processing remains safe, secure and information integrity maintained			
Section 2			
Protected Characteristic	If the proposal/s have a positive or negative impact please give brief details		
Age	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Disability	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Gender reassignment	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Marriage & Civil Partnership	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Pregnancy & Maternity	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Race	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Religion and Belief	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Sex	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Sexual Orientation	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
Other equality groups?	Positive – the principle of conducting a DPIA is based on protecting the information rights of individuals		
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.	<input checked="" type="checkbox"/>
Section 4			
If this proposal is low risk please give evidence or justification for how you reached this decision:			

The principle of conducting a Data Protection Impact Assessment is based on protecting the information rights of all individuals.			
Signed by reviewer/assessor		Date	21/10/2022
<i>Sign off that this proposal is low risk and does not require a full Equality Analysis</i>			
Head of Service Signed		Date	06/01/2023

Appendix 5

DATA PRIVACY IMPACT ASSESSMENT SCREENING

<p>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.</p> <p>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.</p>		
Name of Document:	Data Protection Impact Assessment Policy and Procedure	
Completed by:	Hannah Plowright	
Job title	Data Privacy and Information Governance Manager/Deputy Data Protection Officer	21/10/2022
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	No	

be perceived as being privacy intrusive? For example, the use of biometrics.		
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	
<p>If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt.dataprivacy@nhs.nhs.uk In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.</p>		
Data Privacy approval name:	Hannah Plowright	
Date of approval	21/10/2022	

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

Appendix 6

13.0. Referencing Guidance

The policy was drafted with reference to the following:

- The Data Protection Act 2018
- UK General Data Protection Regulations 2016/679
- Information Commissioners Office Guidance for Data Protection Impact Assessments
- NHS Digital Data Security and Protection toolkit
- National Data Guardian Standards
- Health and Social Care Act 2012
- LPT Data Protection and Information Sharing Policy
- LPT Data Protection and Security Framework

CQC Fundamental Standards – (with effect) 1st April 2015

The **Fundamental Standards** of quality and safety came into effect from 1st April 2015 and replace the 16 **Essential Standards (2010)**.

There are 13 **Fundamental Standards** associated with the quality and safety of care which every staff member must comply with. The Care Quality Commission register, inspect and rate all NHS providers of care to ensure they are demonstrating compliance with the expected **legal minimum standards when delivering patient care**.

Here is a summary of the **standards** that everybody has a right to expect when they receive care, Standard which our care must never fail to achieve.



- Regulation 9 Person-centred care**
The care and treatment of service users must be appropriate, meet their needs and reflect their preferences.
- Regulation 10 Dignity and respect**
Service users must be treated with dignity and respect.
- Regulation 11 Need for consent**
Care and treatment of service users must only be provided with the consent of the relevant person.
- Regulation 12 Safe care and treatment**
Care and treatment must be provided in a safe way for service users.
- Regulation 13 Safeguarding service users from abuse and improper treatment**
Service users must be protected from abuse and improper treatment.
- Regulation 14 Meeting nutritional and hydration needs**
The nutritional and hydration needs of service users must be met.
- Regulation 15 Premises and equipment**
All premises and equipment used by the service provider must be: clean, secure, suitable for the purpose, for which they are being use, properly used, maintained and appropriately located for the purpose for which they are being used.
- Regulation 16 Receiving and acting on complaints**
Any complaint received must be investigated and necessary and proportionate action must be taken in response to any failure identified by the complaint or investigation.
- Regulation 17 Good governance**
Systems or processes must be established and operated effectively to ensure compliance with these regulations.
- Regulation 18 Staffing**
Sufficient numbers of suitably qualified, skilled and experienced persons must be employed.

Regulation 19 Fit and proper persons employed

Persons employed must be of good character, have the qualifications, competence, skills and experience.

Regulation 20 Duty of Candour

Providers are open and transparent with people who use services and other 'relevant persons' in relation to care and treatment.

Regulation 20A Requirement to display performance assessments

When providers have received a CQC inspection for their service, ratings must be displayed legibly at each location delivering a clinical service and on the Trust website.

Every member of staff has a duty to ensure they are demonstrating compliance with the Fundamental Standards, in their day to day practice. If you have any concerns about your ability to demonstrate compliance with these standards, please discuss this with your line manager in the first instance, your Governance Lead, or the Regulation and Assurance team – contact via email lep-tr.compliance@nhs.uk