Leeds and York Partnership
NHS Foundation Trust

DATA PROTECTION POLICY

The key messages the reader should note about this document are:

1. Presents the statutory requirements of the EU General Data Protection Regulation, as enacted in the UK as the Data Protection Act (12018).

2. States what we must do as an organisation and as Trust / NHS employees to comply with the law.

3. States the Trust policy position to enact all Data Protection Principles.

4. States the Trust policy position to enact the ICO 12-Step approach to GDPR compliance.

5. Over-arches the production of other policy / procedural documents in the areas of Information Governance, Data Protection, and Information Security.

This policy/procedure may refer to staff as qualified/registered/professional or other such term to describe their role. These terms have traditionally referred to individuals in a clinical role at band 5 or above. Please note that the use of these terms **may or may not** include nursing associates or associate practitioners (band 4). For clarification on whether a nursing associate or associate practitioner is an appropriate person to take on the identified roles or tasks in this policy/procedure please refer to the job description and job plan for the individual, or local risk assessment.

DOCUMENT SUMMARY SHEET

ALL sections of this form must be completed.

Document title	Data Protection Policy
Document Reference Number	IG-0010
Key searchable words	Data Protection, General Data Protection Regulation
Executive Team member responsible (title)	Chief Financial Officer (as SIRO)
Document author (name and title)	Carl Starbuck Head of Information Governance
Approved by (Committee/Group)	Information Governance Group
Date approved	25/09/2019
Ratified by	Policy & Procedure Group
Date ratified	12/12/2019
Review date	12/12/2022
Frequency of review	At least every three years, or sooner if significant changes to the over-arching legal framework occur.

Amendment detail

Version	Amendment	Reason
0.1	First draft for review	First draft for review

CONTENTS

1. The Policy

On 25th May 2018, the Data Protection Act (1998) was superseded by new EU legislation – the General Data Protection Regulation (GDPR). This was enacted in the UK as the Data Protection Act (2018) (DPA 2018). The UK enactment contained GDPR, plus additional content added by UK Government, e.g. specific sections on Safeguarding & Police / Forensic data processing.

This policy states the Trust's "must does" to embed GDPR / the Data Protection Act (2018) into our work. It will state the Principles to be enacted, and explain their meaning and how they must be applied within the Trust.

In addition to the 7 Data Protection Principles, the ICO's "12 Steps to Implementing GDPR" will also be included, to give a policy mandate for their use when further work on embedding GDPR / DPA 2018 is required, e.g. during the configuration of new or revised services, or the procurement / implementation of new or revised data processing systems or ways of working.

1.1 BREXIT – UK Exit from the European Union

While the UK remains a member state of the European Union, the Data Protection Act (2018) is law as it is the UK enactment of GDPR. If / when the UK leaves the European Union, the Data Protection Act (2018) will remain law.

1.2 Data Protection Act (2018) Principles and their Application in the Trust

Like the 1998 Act before it, the Data Protection Act (2018) sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of our approach to processing personal data.

Note: The 1998 Act had 8 principles, broadly as above but with the 8th principle specifically relating to international transfers of personal data. Under

GDPR & the new Act we regard this as part of our considerations of Integrity and confidentiality (security).

1.2.1 Lawfulness, Fairness, and Transparency

We must identify valid grounds under the Act (known as a 'lawful basis') for collecting and using personal data.

We must ensure that we do not do anything with the data in breach of any other laws.

We must use personal data in a way that is fair. This means we must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

We must be clear, open and honest with people from the start about how we will use their personal data.

1.2.2 Purpose Limitation

We must be clear about what our purposes for processing are from the start.

We need to record our purposes as part of our documentation obligations and specify them in our privacy information for individuals.

We can only use the personal data for a new purpose if either this is compatible with our original purpose, we get consent, or we have a clear obligation or function set out in law.

1.2.3 Data Minimisation

We must ensure the personal data we are processing is:

- adequate – sufficient to properly fulfil our stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – we do not hold more than we need for that purpose.

1.2.4 Accuracy

We should take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact.

We may need to keep the personal data updated, although this will depend on what we are using it for.

If we discover that personal data is incorrect or misleading, we must take reasonable steps to correct or erase it as soon as possible.

We must carefully consider any challenges to the accuracy of personal data.

1.2.5 Storage Limitation

We must not keep personal data for longer than we need it.

We need to think about – and be able to justify – how long we keep personal data. This will depend on our purposes for holding the data.

We need a policy setting standard retention periods wherever possible, to comply with documentation requirements.

We should also periodically review the data we hold, and erase or anonymise it when we no longer need it.

We must carefully consider any challenges to our retention of data. Individuals have a right to erasure if we no longer need the data.

We can keep personal data for longer if we are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Note: All records retention and disposal in the NHS is dictated by the Records Management Code of Practice for Health & Social Care.

1.2.6 Integrity & Confidentiality (Security)

A key principle of the Act is that we process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.

Doing this requires us to consider things like risk analysis, organisational policies, and physical and technical measures.

We also have to take into account additional requirements about the security of our processing – and these also apply to data processors.

We can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to our circumstances and the risk our processing poses.

Where appropriate, we should look to use measures such as pseudonymisation and encryption.

Our measures must ensure the 'confidentiality, integrity and availability' of our systems and services and the personal data we process within them.

The measures must also enable us to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

We also need to ensure that we have appropriate processes in place to test the effectiveness of our measures, and undertake any required improvements.

1.2.7 Accountability

Accountability is one of the data protection principles - it makes us responsible for complying with the GDPR / DPA 2018 and says that we must be able to demonstrate our compliance.

We need to put in place appropriate technical and organisational measures to meet the requirements of accountability.

There are a number of measures that we can, and in some cases must, take including:

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out Data Protection Impact Assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a Data Protection Officer; and
- adhering to relevant codes of conduct and signing up to certification schemes.

Accountability obligations are ongoing. We must review and, where necessary, update the measures we put in place.

If we implement a privacy management framework this can help us embed our accountability measures and create a culture of privacy across our organisation.

Being accountable can help us to build trust with individuals and may help us mitigate enforcement action.

1.3 12 Steps to Implementing GDPR

In May 2017, the Information Commissioner's Office published a "12 Step" approach to enable organisations to become ready for the roll-out and implementation of the General Data Protection Regulation. This formed the basis for a number of workstreams within the Trust as the enactment of the new law approached.

Although these steps were a pre-cursor to the implementation of the Data Protection Principles outlined in 1.2 above, they are documented here in

policy to give a mandate for their use when further work on embedding GDPR / DPA 2018 is required, e.g. during the configuration of new or revised services, or the procurement / implementation of new or revised data processing systems or ways of working.

1.3.1 Awareness

We should make sure that decision makers and key people in our organisation are aware that the law has changed to GDPR / DPA 2018. We need to appreciate the impact this is likely to have.

1.3.2 Information We Hold

We should document what personal data we hold, where it came from and who we share it with. We may need to organise an information audit.

1.3.3 Communicating Privacy Information

We should review our current Privacy Notice(s) and put a plan in place for making any necessary changes in time for GDPR / DPA 2018 implementation.

1.3.4 Individuals' Rights

We should check our policies & procedures to ensure they cover all the rights individuals have, including how we would delete personal data or provide data electronically and in a commonly used format.

1.3.5 Subject Access Requests

We should update our procedures and plan how we will handle requests within the new timescales and provide any additional information.

1.3.6 Lawful Basis for Processing Personal Data

We should identify the lawful basis for our processing activity in the GDPR / DPA 2018, document it and update our Privacy Notice(s) to explain it.

1.3.7 Consent

We should review how we seek, record and manage consent and whether we need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

1.3.8 Children

We should start thinking now about whether we need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

1.3.9 Data Breaches

We should make sure we have the right procedures in place to detect, report and investigate a personal data breach.

1.3.10 Data Protection by Design and Data Protection Impact Assessments

We should familiarise ourselves now with the ICO's code of practice on Data Protection Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in our organisation.

1.3.11 Data Protection Officers

We should designate someone to take responsibility for data protection compliance and assess where this role will sit within our organisation's structure and governance arrangements. We should consider whether we are required to formally designate a Data Protection Officer.

Note: The Head of Information Governance was formally appointed as the Trust Data Protection Officer.

1.3.12 International

If our organisation operates in more than one EU member state (i.e. we carry out cross-border processing), we should determine our lead data protection supervisory authority. Article 29 Working Party guidelines will help us do this.

Note: The Trust operates solely within the UK, and as such our lead data protection supervisory authority is:-

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Fax: 01625 524510

2 Appendices

None.

PART B

3 IDENTIFICATION OF STAKEHOLDERS

The table below should be used as a summary. List those involved in development, consultation, approval and ratification processes.

Stakeholder	**Level of involvement**
Information Governance Group (comprising) • Head of Information Governance / DPO • IG Support Officer • Chief Information Officer • Head of Performance Management & Informatics • Head of IT Service Delivery • ICT Service Desk Manager / RA Manager • ICT Network Support Manager	Consultation
Staffside representative	Consultation
Information Governance Group	Approval
Policy & Procedure Group	Ratification

4 REFERENCES, EVIDENCE BASE

Data Protection Act (2018)

EU General Data Protection Regulation

ICO – Guide to the General Data Protection Regulation (GDPR)

ICO – Preparing for the General Data Protection Regulation (GDPR) – 12 Steps to Take Now

Records Management Code of Practice for Health & Social Care (2016).

5 ASSOCIATED DOCUMENTATION (if relevant)

- IG-0001 – Information Governance Policy
- IG-0002 – Health Records Policy
- IG-0003 – Confidentiality Code of Conduct
- IG-0004 – Forensic Readiness Policy
- IG-0005 – Freedom of Information Procedure
- IG-0006 – Data Quality Policy
- IG-0007 – Corporate Records Management Guidance
- IG-0008 – Data Protection Act - Subject Access Request Procedure
- IG-0009 – Safe Haven Guidance

- IT-0001 – Encryption Policy
- IT-0002 – Internet Use Policy

- IT-0003 – Email Use Policy
- IT-0004 – Network Security Policy
- IT-0005 – Portable Computing Device Policy
- IT-0006 – Recording Deceased Service Users on the PARIS System
- IT-0007 – PARIS Data Collection and Input Procedure
- IT-0008 – Information Security Policy
- IT-0009 – Supplier Support Access Agreement Procedure
- IT-0010 – Mobile & Smartphone Communications Policy

- IG Group Terms of Reference

6 STANDARDS/KEY PERFORMANCE INDICATORS (if relevant)

Not relevant. As this is an over-arching policy document, Key Performance Indicators will be monitored against procedural documents covering the workstreams carried out under this policy's umbrella.

7. EQUALITY IMPACT

The Trust has a duty under the Equality Act 2010 to have due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations between people from different groups. Consideration must be given to any potential impacts that the application of this policy/procedure might have on these requirements and on the nine protected groups identified by the Act (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, gender and sexual orientation).

Declaration: The potential impacts on the application of this policy/procedure have been fully considered for all nine protected groups. Through this process I have not identified any potential negative impacts for any of the nine protected groups.

Print name: Carl Starbuck

Job title: Head of Information Governance

Date: 16/09/2019

If any potential negative impacts are identified the Diversity Team must be contacted for advice and guidance: email; diversity.lypft@nhs.net.

CHECKLIST

To be completed and attached to any draft version of a procedural document when submitted to the appropriate group/committee to support its consideration and approval/ratification of the procedural document.

This checklist is part of the working papers.

	Title of document being newly created / reviewed:	Yes / No/
1.	**Title**	
	Is the title clear and unambiguous?	✓
	Is the procedural document in the correct format and style?	✓
2.	**Development Process**	
	Is there evidence of reasonable attempts to ensure relevant expertise has been used?	✓
3.	**Content**	
	Is the Purpose of the document clear?	✓
5.	**Approval**	
	Does the document identify which committee/group will approve it?	✓
6.	**Equality Impact Assessment**	
	Has the declaration been completed?	✓
7.	**Review Date**	
	Is the review date identified?	✓
	Is the frequency of review identified and acceptable?	✓
8.	**Overall Responsibility for the Document**	
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	✓

Name of the Chair of the Committee / Group approving			
If you are assured this document meets requirements and that it will provide an essential element in ensuring a safe and effective workforce, please sign and date below and forward to the chair of the committee/group where it will be ratified.			
Name	*Carl Starbuck* *Head of Information Governance*	Date	*17/09/2019*
Name of the chair of the Group/Committee ratifying			
If you are assured that the group or committee approving this procedural document have fulfilled its obligation please sign and date it and return to the procedural document author who will ensure the document is disseminated and uploaded onto Staffnet.			
Name	*Cath Hill* *Associate Director for Corporate Governance*	Date	*12/12/2019*