NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Information Governance Framework Policy

Policy Number	**IG/Pol/015**
Target Audience	**All staff including permanent, temporary, contractors, learners in practice, apprentices and volunteers**
Approving Committee	**Corporate Clinical Policy Group**
Date First Approved	**May 2021**
Last Full Review Date	**New Policy**
Next Full Review Date	**May 2024**
Policy Author	**Information Governance and Records Manager**
Version Number	**1.0**

Applicable Statutory, Legal or National Best Practice Requirements	Data Protection Act 2018, c.29. Equality Act 2010, c. 15 Freedom of Information Act 2000, c.36 Human Rights Act 1998, c.42 Information Commissioner's Office 2018, Guide to the General Data Protection Regulation (GDPR) National Data Guardian 2020, The Caldicott Principles NHS Digital 2018 Data Security Standard 4 Protection of Freedoms Act 2012, c.9

The Trust is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	28/10/2020	S. Ramsdale	First draft
0.2	March 21	DIGIT members	See consultation section
0.3	April 21	Mary Corkery	Comments made
0.4	April 21	S. Ramsdale	Updated following comments
0.5	May 2021	Corporate Clinical Policy Group	Approved subject to minor amendments and final chair approval
0.6	May 2021	S. Ramsdale	Amendments completed
1.0	May 2021	S. Arkwright	Approved by chair action

Does this policy impact/potentially impact on: • **Staff** • **Patients** • **Family Members** • **Carers** • **Communities**	**Yes**	**Please contact the Trust's Equality & Inclusion Manager at:** **Email: ruth.besford@nhs.net**
	No	**Please sign and date below:** **Name:** **Email Address:** **Date:**

Education & Professional Development Question

In order to ensure that any training requirements are discussed and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements. Please answer the following question by entering a cross in the box below:

	Yes	No
Does this document have any additional training requirements or implications?		x

Contents

The following appendices can be accessed electronically by clicking on the following link:

1 Introduction

This policy aims to detail how Bridgewater Community Healthcare Foundation Trust (hereafter the Trust) supports its staff in handling personal information within a legal framework to enable them to undertake their jobs. Under data protection legislation, organisations that process personal data are accountable for, and must be able to demonstrate their compliance with the legislation.

The formal framework that leaders of all health and social care organisations should commit to is set out in the National Data Guardian's ten data security standards. These are the basis of the Data Security and Protection Toolkit (DSPT) that health and social care organisations must use to assess their information governance performance.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information Governance Management
- Clinical Information assurance for Safe Patient Care
- Confidentiality and Data Protection assurance
- Corporate Information assurance
- Information Security assurance
- Secondary use assurance
- Respecting data subjects' rights regarding the processing of their personal data
- Freedom of Information rights.

The arrangements set out in this and related policies and procedures are intended to achieve this demonstrable compliance. To support the information governance framework, relevant Trust policies and procedures are directly referenced throughout this document.

The Information Governance policy produced by NHS England and NHS Innovation has been used as a basis for this policy.

1.1 Objective

This policy is to inform all Trust staff of their Information Governance responsibilities and the management arrangements, and that other policies are in place to ensure demonstrable compliance within an information governance framework.

The policy sets out how data is:

- Held securely and confidentially
- Processed fairly and lawfully
- Obtained for specific purpose(s)

- Recorded accurately and reliably
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully.

To protect the Trusts information assets from all threats, whether internal or external, deliberate or accidental, the Trust will ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information governance training will be available to all staff
- All information governance breaches, actual or suspected, will be reported to, and investigated by the Information Governance team in conjunction with the Data Protection Officer.

1.2 Scope

This policy, together with the associated standards, is aimed at all staff, including permanent, temporary, contractors, learners in practice, apprentices and volunteers, who manage and handle personal information/data.

All staff must adopt working practices so they can be considered a 'personal safe haven', essentially a safe pair of hands for personal, sensitive or confidential information.

This policy relates to all information held or due to be held by the Trust or those who process information on behalf of the Trust.

2 Definitions

The definitions applicable to this document are as follows:

Name	Definition
Personal Data	Personal data is defined in the General Data Protection Regulation (GDPR) as: "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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 data, 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".

Name	Definition
Natural Persons	Natural person is a person who is alive. Note: a health record for a deceased person may contain personal information of a natural person and this should be considered in the event of a data breach.
Data Subject	The identified or identifiable living individual to whom personal data relates.
Special Category Data	The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection: • Personal data revealing racial or ethnic origin • Personal data revealing political opinions • Personal data revealing religious or philosophical beliefs • Personal data revealing trade union membership • Genetic data • Giometric data (where used for identification purposes); • Data concerning health • Data concerning a person's sex life • Data concerning a person's sexual orientation.
Biometric data	Facial imaging and fingerprint data are just two examples, but these are not exhaustive. Many other types of physical, physiological or behavioural 'fingerprinting' fall within the definition. Examples of physical or physiological biometric identification techniques: • Facial recognition • Fingerprint verification • Iris scanning • Retinal analysis • Voice recognition • Ear shape recognition.
Safe Haven	The term Safe Haven refers to either a secure physical location or an agreed set of administrative arrangements for ensuring the safety and secure handling of confidential patient information.
Data Controller	An organisation that determines the purpose, category and the manner in which personal data is processed.
Data processor	A person or organisations that follows instructions from someone else regarding the processing of personal data.
Tracking and Tracing	A record of movement of the record to ascertain whereabouts of the information at all times.

Name	Definition
Information Asset	*"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles."* (National Archives 2017)
Record of Processing Activities (ROPA) or Data flow/s	Article 30 of GDPR – Records of processing activities. It is both controller and processors responsibility to record, who and why you are sharing information what is the purpose etc.
Subject Access Request (SAR)	The right of access (Article 12 GDPR), commonly referred to as subject access requests, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully. (ICO 21)
Data Protection impact Assessment (DPIA)	A process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.
Caldicott Guardian	A senior person responsible for protecting the confidentiality of a patient and service-user information and enabling appropriate information-sharing.
Data Breach	A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also covers **not** disclosing information when it should have been.
Processing (of information)	Art.4(2) "Processing" means any operation or set of operations performed upon personal data or 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.

3 Abbreviations

The abbreviations applicable to this document that are not explained elsewhere are as follows:

IT	Information Technology
DPIA	Data Protection impact Assessment
ROPA	Record of Processing Activities
SAR	Subject Access Request
ICO	Information Commissioners Office
GDPR	General Data Protection Regulation
DSPT	Data Security and Protection Toolkit
SIRI	Serious Incident Requiring Investigation
IG	Information Governance
SIRO	Senior Information Risk Owner
DPO	Data Protection Officer
IAOs	Information Asset Owners
DIGIT	Digital, Information Governance and Information Technology Group
PPDR	Performance and Personal Development Review
FOIA	Freedom of Information Act
TOR	Terms of Reference
CNIO	Clinical Informatics Chief Nurse
NDG	National Data Guardian

4 Other Relevant Procedural Documents

Policies and procedures directly referenced with relevant section are:

Corporate Records (including Document Management) Policy

IT Asset Policy

Acceptable use IT Policy

Health Records Policy

Data Encryption Policy

Records Management – Storing and Movement of Records Policy

Mandatory Training & Induction Policy

Performance and Personal Development Review Policy

Subject Access / Access to Health Records Policy

Procurement Policy

Additional Trust policies that are also linked and why they are linked are explained below:

Policies and Procedure	Description and content
Data Protection and Confidentiality Policy	This policy is directly linked to the Information Governance Framework (this policy). The Data Protection and Confidentially Policy has details on our responsibilities as an organisation on how we should process, share and disclose information within a legal framework.
Incident Reporting Policy	The Trusts Risk Management Reporting System (Ulysses) process and stores all the Trusts incidents, all incidents are to be logged via this system. Relating to Information Governance, this is when a **data breach** occurs that may affect the "rights and freedoms" of the individual or individuals. A data breach incident that is deemed serious is to be reported to the Information Commissioners Office (ICO) within 72 hours, this is covered within this policy. The policy is also supported by the Procedure for serious data breach when on call. Appendix 5 has a template that is distributed when incidents that are not deemed serious i.e. less than 3.
Incident Investigation Procedure	This procedure supports the Incident Management Policy. As with all serious incidents data breaches need to be investigated and lessons learned to prevent reoccurrence. The IG team report on these serious incidents and undertaken or offer expert advice in relation to these Serious Incidents Requiring Investigation (SIRI).

Risk Management Framework and Risk Assessment and Risk Register Process Guideline	Sets out how the Trusts manage risk within the organisation. Information Governance risks may include any known privacy concerns or known risks by Information Asset Owners regarding management of their information assets.
NHSmail - Acceptable use policy	This document explains how the NHSmail service should be used. It is your responsibility to ensure you understand and comply with this policy. It ensures that: • You understand your responsibilities and what constitutes abuse of the service. • Computers and personal data are not put at risk. • You understand how NHSmail complies with the GDPR (Regulation (EU) 2016/679) by reading the Transparency Information.

5 Roles and Responsibilities

5.1 Chief Executive

Overall accountability for procedural documents across the organisation lies with the Chief Executive as the Accountable Officer.

The Accountable Office has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements and adhering to guidance issued in respect of information governance and procedural documents.

5.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is the Board Member who has overall responsibility for Information Risk Management in the Trust. The responsibilities of the SIRO are:

- Take overall ownership of the organisation's Information Risks
- Understand how the strategic business goals and how other NHS organisation's business goals may be impacted by information risks, and how those risks may be managed
- Implement and lead the Information Governance Risk Assessment and Management processes

- Sign off and take accountability for risk-based decisions and reviews in regards to the processing of personal data

- Advise the Board on the effectiveness of information risk management across the Trust

- Receive training as necessary to ensure they remain effective in their role as SIRO. This will mean attending external training on a 3 year basis.

The SIRO will report to the Quality and Safety Committee on information risks and through the Statement of Internal Controls following assurance from the Information Asset Owners. The SIRO is the Director of Finance. The Deputy SIRO is the Assistant Director for IT.

5.3 Caldicott Guardian

The Caldicott Guardian is the Chief Nurse. The Deputy Caldicott Guardian is the Deputy Chief Nurse.

They will:

- Ensure that the Trust satisfies the highest practical standards for handling patient identifiable information

- Facilitate and enable appropriate information sharing and make decisions on behalf of the Trust following advice on options for lawful and ethical processing of information, in particular in relation to disclosures

- Represent and champion Information Governance requirements and issues at Board level

- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff

- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within and outside the NHS.

5.4 Data Protection Officer

The Data Protection Officer (DPO) for the Trust is held by the Trust Secretary. The DPO reports directly to the Board about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data. With the support of their office, the DPO will:

- Provide advice to the organisation and its employees on compliance obligations with data protection law

- Advise on when data protection impact assessments are required
- Monitor compliance with data protection law and organisational policies in relation to data protection law
- Co-operate with, and be the first point of contact for the Information Commissioner
- Be the first point of contact within the organisation for all data protection matters
- Be available to be contacted directly by data subjects
- Take into account information risk when performing the above
- Will be the key contact in the event of a data breach.

5.5 Assistant Director of Information Technology

The Assistant Director of Information Technology (IT), supported by the Head of IT and their teams, are responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure the Trust systems and infrastructure remain compliant with data protection legislation.

They are responsible for ensuring that all of the Trust electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

5.6 Information Asset Owners

Information Asset Owners (IAOs) will:

- Lead and foster a culture that values, protects and uses information for the benefit of patients
- Know what information comprises or is associated with their asset(s) and understand the nature and justification of information flows to and from the asset
- Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy
- Understand and address risks to the asset and provide assurance to the SIRO
- Ensure there is a legal basis for processing and for any disclosures
- Refer queries about any of the above to the Information Governance team

- Ensure all information assets they are owner for are recorded on the Information Asset Register

- Undertake specialist information asset external training on a 3 yearly basis.

5.7 Information Governance and Records Manager

With the support of the Information Governance (IG) team, the Information Governance and Records Manager will:

- Maintain an awareness of information governance issues within the Trust

- Keeps up to date with changes in legislation to ensure the Trust remains compliant

- Review and update the information governance policy in line with local and national requirements

- Work with IAO's and project managers to complete a DPIA and recommend any areas of risk

- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis

- Ensure that line managers are aware of the requirements of the policy

- Work with the Caldicott Guardian, SIRO and DPO functions to ensure organisational authority and awareness regarding issues relating to data protection or confidentiality concerns.

5.8 Borough Directors

Borough Directors supported by their managers are responsible for:

- The implementation of IG and IT related policies and where indicated the creation of supporting procedures, ensuring these are embedded within the service and developing, implementing and managing robust IT security arrangements in line with best industry practice

- Effective management and security of the Trust's Assets including IT resources, for example, infrastructure and equipment

- Developing and implementing a robust IT Disaster Recovery Plan

- Ensuring that IT security levels required by the NHS Statement of Compliance are met

- Ensuring the maintenance of all firewalls and secure access servers are in place at all times

- Acting as the Information Asset Owner with specific accountability services that are operated by corporate and clinical work force, e.g. personal computers, laptops, personal digital assistants and related computing devices, held as an Information asset

- Work with the Information Governance team and DPO as appropriate regarding matters relating to data and IT security.

5.9 Service/Clinical Managers

Service/Clinical Managers will:

- Ensure all staff are compliant with the Data Security Awareness Level 1 training

- Ensure Information Governance and Data Security is embedded within the teams by having it as a regular agenda item at team meetings

- Manage and investigate data breaches and ensure lessons are learned.

5.10 Staff with elevated access

Staff with elevated access to IT/Information systems, including clinical systems and health records will be held accountable to the highest standards of use; they will be subject to higher monitoring and will have subsequent enhanced contract agreements.

"A system administrator is typically responsible for installing, configuring and maintaining hardware and software infrastructure. Systems administrators by nature of their role have elevated rights compared to a normal user." (NHS Digital – Data Security Standard 4 (2018).

Specific staff with access to personal information including those in areas elevated access, information asset owners and information asset administrators will have training as per training needs analysis which will be reviewed annually (see section 7.9 Training).

5.11 Digital, Information Governance and Information Technology Group

Digital, Information Governance and Information Technology Group (DIGIT) oversees this Framework and the policies referred to within it, as well as any agreed information governance improvement programmes.

5.12 All Staff

It is the responsibility of each employee to adhere to this policy and all associated information governance, IT and information security policies and procedures.

Staff will receive instruction and direction regarding the policy from several sources:

- Mandatory training
- Information Governance Team (IG team)
- Policy/strategy and procedure processes
- Line manager/director
- Specific training course/s
- Other communication methods, for example, team meetings; staff intranet/bulletin/corporate emails.

All staff must make sure that they use the organisation's IT systems appropriately and adhere to the Acceptable use (IT) Policy, the policy includes user obligations.

6 Equipment List

Not applicable.

7 Information Governance Framework

The Trust has multiple associated information systems within the organisation, as well as information held outside the organisation. The Information governance framework ensures that personal information meets the Trusts regulatory and legal obligations. This means information will be:

- Held securely and confidentiality
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically, and shared/disclosed
- Ensure the data rights of individuals are upheld.

The Caldicott principles should always be considered when handling personal information. There are multiple policies directly associated with this policy to ensure the Trust has a robust information governance framework, these referenced throughout this document.

7.1 Personal Information

The definition of "personal data" is *"any information relating to an identified or identifiable natural person – i.e. living individuals. Personal data has different data categories for example name and date of birth is personal information, information on sexual health is deemed special category data and requires extra measures"* (GDPR 2018)

Examples of personal information and special category data can be found in this policy in section 2 - Definitions.

The Corporate Records (including document management) policy has information how certain types of records, information and documents should be, named and categorised before filing and retaining. The classification of information is called metadata and has standard elements, which are designed to form the basis for the description of all information.

The policy also includes security classification standards this is in addition to any metadata needed to manage information through the information lifecycle; all information should possess a security classification.

You put things in simple terms to manage information you know what the information is, describe it, and name it; only then can you know how to handle it. The Trust retention schedule has an index on information the Trust holds this can be found here.

7.2 Held securely and confidentially

All personal information including certain business or corporate information needs to be stored, transmitted and only accessed or handled when necessary. This means information needs to be safeguarded when stored, accessed or when it enters or leaves the organisation whether this is by fax, post, verbally, email or other means.

The Information Asset and System Audit Policy includes what is expected of IAO'S and information asset administrators, full details of roles and responsibilities here. In brief the IAO is responsible for ROPA and knowing their "data flow/s" in and out of their asset. An example of an incoming data flow is and receiving a health record by post another would be receiving a health record via email. They need to provide evidence on who has access to their asset, and why, along with the lawful basis of sharing any information.

The IT Asset Policy and the Acceptable use IT policy has information on what IT equipment is used within the Trust and what is expected of the users (staff) when using this equipment to ensure the information held is secured at all times.

The Information Security Policy has information on transfers of electronic information and how the protection of Information Assets. The Data Encryption Policy has the Trusts approach on how to secure information within the IT assets.

The Records Management – Storing and Movement has records policy has core standards on storing and transferring records within a paper format. It includes "tracking and tracing" guides on how records/information needs to be secured at all times; this is for both electronic and paper records. Tracking of electronic information is sometimes easier than that of paper records as paper records do not have a digital audit log a manual process has to be adopted. This policy also has the retention schedule for each of the record types.

The Records Management – Storing and Movement also includes the governance required when there is bulk transfers of information, including electronic transferred of 50 or more records. The bulk data transfer form (Appendix 6) is a good approach in providing documented evidence of transferring information regardless of size and should be utilised.

Appendix 1 – Guidance for sending by FAX
Appendix 2 – Guidance on how to handle post (in and out)
Appendix 3 – Guidance on telephone calls or verbal communication
Appendix 4 – Other media/communication devices

7.3 Obtained fairly and lawfully

Article 5(1) of the GDPR says: *"1. Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')".*

Lawfully is the grounds in which you are collecting the personal information. As a health organisation our legal basis for processing is normally to carry out "public task" ie as an official NHS authority to carry out the task of caring for people. It could also be "vital interest" ie to prevent harm. In other words we do not need consent to process information but we have to do it fairly. We have to be open and honest on how we are using and sharing the information we are collecting.

The Data Protection and Confidentially Policy has details on our responsibilities as an organisation on how we control information and how we do this fairly. It also includes how children have the right to be informed.

7.4 Recorded accurately and reliably

The core characteristics of accurate information are:

- **Authentic** – i.e. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed

- **Reliable** – i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records

- **Integrity** – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified

- **Useable** – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record.

The Trust Health Records Policy has the Trusts approach to the quality of information captured is accurate and reliable, the policy sets out how we:

- Use a standardised structure for the contents of records
- Standards when creating a corporate health records
- Ensure documentation reflects the continuum of care, that all care is person centred and that care records are viewable in chronological order
- Provide a clearly written care plan when care is being delivered by several members of the team, and we ensure that records are maintained and updated, and shared with everyone involved
- Correction of errors
- Audit process

7.5 Used effectively and ethically, and shared/disclosed

Personal data can only be shared if there is a clear legal basis to do so or if the data subject has given their clear consent. If you are required to share personal data you should be clear about the reasons for sharing the data, and what you intend to achieve by doing so. As stated early the legal basis for processing and sharing information is based on health and social care to perform a “public task”, meaning we do not share information based on consent, it is based on care needs.

The Data Protection and Confidentially Policy has details on our responsibilities as an organisation on how we should share and disclose information within a legal framework.

7.6 The Eight Caldicott Principles

The eight Caldicott principles should be considered for all health and social care services. (NDG 2021) These are:

Principle 1: Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law Every use of confidential information must be lawful

All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

The Data Protection and Confidentially Policy has the Trust approach to how we process information appropriately this along with the Trusts DPIA template that needs to be completed before every new or change in processing (sharing) of information.

Under the GDPR, we have a have an obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities. Privacy by design should be a key consideration in the early stages of any project and should continue throughout its lifecycle. This allows us to minimise privacy risks and builds trust. By designing projects, processes, products and systems with privacy in mind at the outset can lead to benefits.

The Data Protection and Confidentially Policy also has details on how as Trust we are control the processing of information. We inform, protect and share and minimise our information.

The Trust's Privacy Notice for patients and the Staff Privacy Notice information explains how we process personal information in the Trust. It is kept up to date, and complies with the Information Commissioner's Office (ICO) Code of Practice (2018).

7.7 Data Breaches and Data Incidents

One of the requirements of the GDPR is that the Trust must use appropriate technical and organisational measures, to ensure that personal data is processed in a manner to ensure the appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Breaches can be categorised as:

- Confidentiality breach – unauthorised or accidental disclosure of, or access to personal data
- Availability breach – where there is an accidental or unauthorized loss of access to or destruction of, personal data
- Integrity breach – where there is an unauthorised or accidental alteration of personal data.

Data breaches can have a range of significant adverse effects on individuals which can result in physical, material or non-material damage.

As a Trust we have a duty to report a serious personal data breach to the ICO. A breach must be notified to the ICO within 72 hours therefore a data breach which involves a group of individuals and or vulnerable individual that is likely to result in a high risk to the rights and freedoms of the individual should be reported to the manager and the Information Governance Team immediately.

Further information on serious data breaches can be found in the Incident Reporting Policy.

Following a data breach the Trust must inform those individuals without undue delay. All data breaches regardless of severity are to be reported on the Trust reporting system and the Incident Reporting Policy is to be followed.

All data incidents are monitored by the Information Governance Team.

7.8 Overseas Transfers

The Trust does not routinely transfer any person identifiable information outside of the UK. If a member of staff is asked to transfer personal data outside the UK, they should contact the Information Governance Team on BCHFT.IG@nhs.net who will provide advice and guidance on a case by case basis. Through the Procurement and DPIA process any transferred will be highlighted.

7.9 Training

Staff will undertake mandatory data security awareness training level 1 annually.

In addition to the annual data security awareness training the Trust Board, SIRO and Caldicott guardian and deputies, along with IAO and IAA will undertake further training every 3 years. Those staff identified in specialist roles will identify their training needs though their annual Performance and Personal Development Review (PPDR) process.

The data protection spot check questionnaire will be distributed to all staff annually. This will help identify any gaps in knowledge and identify any training needs.

7.10 Freedom of Information Act 2000 (FOIA)

FOIA is covered under the Information Governance Framework. The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Public authorities include government departments, local authorities, the NHS, state schools and police forces.

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

It is important to remember, that while personal information would be exempt under section 40 of the FOIA and should not be provided, data should be kept accurate, relevant and up to date. Records should be classified appropriately, classification can be found in the Corporate Records Policy.

The Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a public authority holds about them, they should make a data protection subject access request.

8 Consultation

Key individuals/groups involved in the development of the document to ensure it is fit for purpose once approved.

Name	Designation
DIGIT Members as per Terms of Reference (TOR)	Associate Director: Quality Governance Director of Finance/ Senior Information Risk Owner Responsible Non-Executive Director Assistant Director For IT/Deputy SIRO Deputy Director Information & Clinical Performance Data Protection Officer Information Governance and Records Manager Senior Information Governance Officer Head of IT Head of Data Security Clinical Informatics Chief Nurse (CNIO) Registration Authority & Training Lead Head of Procurement Director of Operations / Nominated Deputy – Warrington Director of Operations / Nominated Deputy – Halton & St Helens Director of Operations / Nominated Deputy – Dental Director of Operations / Nominated Deputy – Health and Justice Education & Professional Development Lead Human Resources
Mary Corkery	Policy Officer
Razia Nazir	Knowledge and Library Services Manager
Ruth Besford	Equality and Inclusion Manager
Corporate Clinical Policy Group	

9 Dissemination and Implementation

9.1 Dissemination

The Information Governance and Records Manager will disseminate this policy to Borough Directors for disseminating to staff. This policy will be made available on the Trust intranet and public facing website. The policy will be published on the in the bulletin and team brief and sent out via global e-mail.

9.2 Implementation

Borough Directors will ensure all Trust staff adheres to this policy.

All staff will be made aware of their personal and organisational responsibilities regarding information governance through the Trust mandatory training program, local induction and monitoring audits.

New employees will be made aware of this policy through the Induction process.

10 Process for Monitoring Compliance and Effectiveness

The core aspects outlined within the policy are monitored through the Trusts Information Governance audit program, which is both internally and external to the Trust for example the DSPT.

11 Standards/Key Performance Indicators

95% of Staff will undertake mandatory data protection and security training level 1 annually.

Serious data breaches are reported to the ICO within 72 hours of identification.

12 References

Data Protection Act 2018, c.29. [online]. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents

Equality Act 2010, c. 15 [online]. Available at: http://www.legislation.gov.uk/ukpga/2010/15/contents

Freedom of Information Act 2000, c.36 [online]. Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents

Human Rights Act 1998, c.42 [online]. Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents

Information Commissioner's Office 2018, Guide to the General Data Protection Regulation (GDPR) [online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf found here https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

National Archives 2017, What is an information asset? [webpage]. Available at: https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

National Data Guardian (NDG) 2020, The Caldicott Principles [online]. Available at: https://www.gov.uk/government/publications/the-caldicott-principles
NHS Digital 2018 Data Security Standard 4 [webpage]. Available at: file:///C:/Users/MARYCO/Downloads/Data%20Security%20Standard%2004%20big%20picture%20guide%20Social%20Care.pdf

NHS England and NHS Innovation (no date) [online]. Available at: https://www.england.nhs.uk/ourwork/innovation/

NHSmail (no date) Acceptable Use Policy [online]. Available at: https://portal.nhs.net/Home/AcceptablePolicy

NHSmail Transparency / Fair Processing Information 2018, v.4 [webpage]. Available at: https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/NHS+Digital+(NHSmail+Live+Service)+Transparency+Information.pdf

Protection of Freedoms Act 2012, c.9 [online]. Available at: https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Records Management Code of Practice 2020, A guide to the management of health and care records [webpage]. Available at: https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_Code_of_Practice_2020_3.pdf

UK Caldicott Guardian Council 2020, The Eight Caldicott Principles [webpage]. Available at: https://www.ukcgc.uk/manual/principles