Data Protection Policy

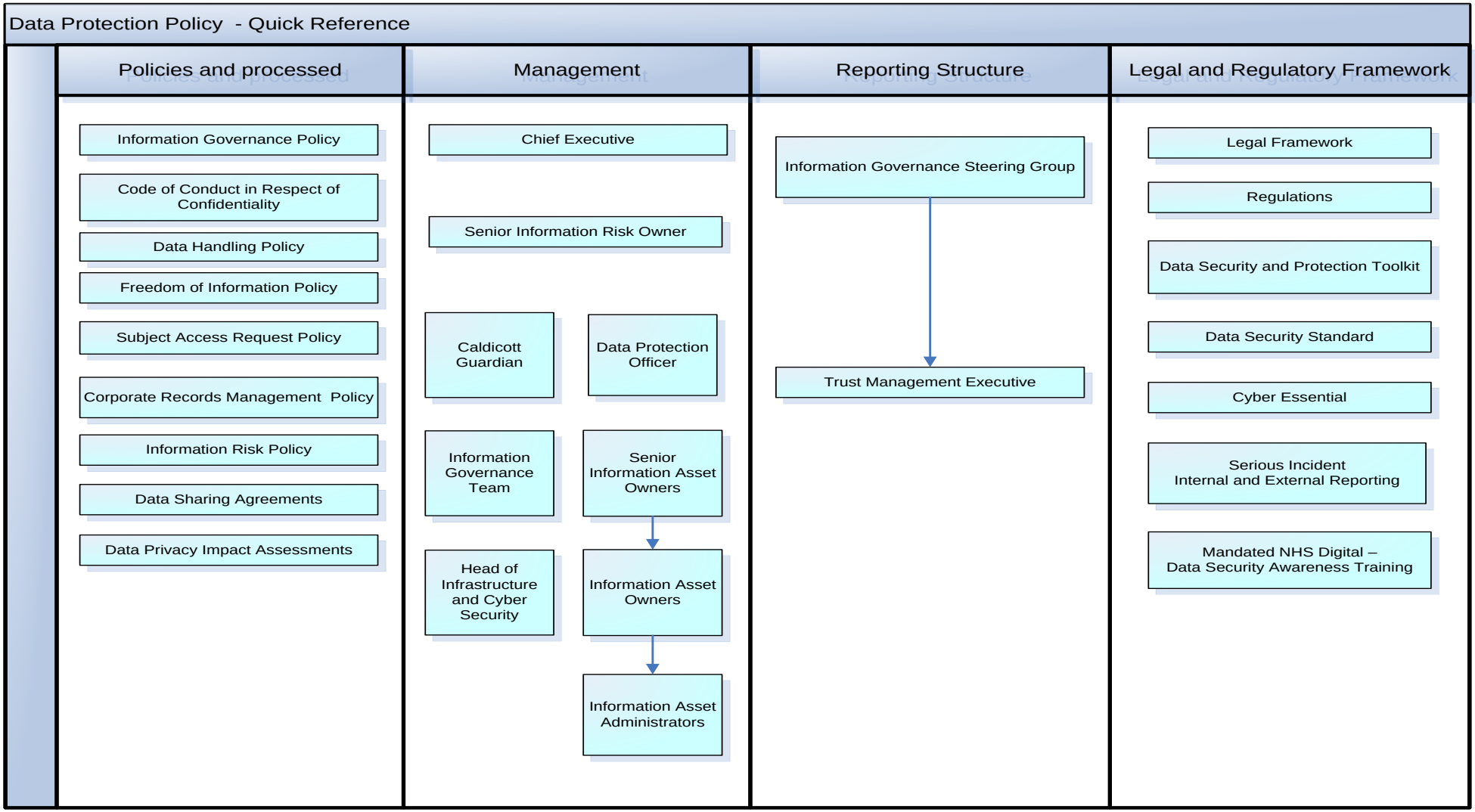
Department / Service:	Information Governance
Originator:	Information Governance Manager
Accountable Director:	Chief Finance Officer (Senior Information Risk Owner – SIRO)
Approved by:	Information Governance Steering Group Trust Management Executive (TME)
Date of approval:	30th September 2021
Review Date: **This is the most current document and should be used until a revised version is in place**	30th March 2025
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All departments
Target staff categories	All Trust staff/contractors/volunteers

Policy Overview:
The relevant Data Protection Regulations and how they affect the Trust. How these regulations affect you as a Trust Employee, and guarantee your rights, and our patient's rights as data subjects. Roles and responsibilities for compliance and notification.

Latest Amendments to this policy:
September 2021 – New document approved. Total re-write to align all Information Governance policies July 2024 – Document extended for 6 months whilst documents are reviewed in line with new Data Security and Protection toolkit

Contents

Quick Reference Guide



1. Introduction

Worcester Acute Hospitals NHS Trust is committed to compliance with the Data Protection Act 2018 (DPA18) and will follow procedures that aim to ensure that all employees, contractors, agents, elected members, partners or other service providers of the Trust are fully aware of and abide by their duties and responsibilities under the DPA18.

The Trust will ensure that personal data is handled, legally, securely, efficiently and effectively and in accordance with the principles of the DPA18 (see paragraph 5.2 below).

In order to operate efficiently the Trust will collect and use data relating to patients receiving care and the people with whom it collaborates including members of the public, current, past and prospective employees, suppliers and other visitors. In addition, it may be required by law to collect and use data in order to comply with the statutory requirements of the Department of Health, NHS England, NHS Digital and other government departments.

All personal data, regardless of how it is collated, recorded, utilised and disposed of, whether on paper, by computer or other recording material, will be handled by the Trust within the safeguarding principles of the DPA18 and Information Governance frameworks issued by the Department of Health.

2. Scope of this document

This policy applies to all employees working in the NHS, including temporary staff such as all contractors, voluntary staff, and students.

Employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. This duty continues after termination of employment.

3. Definitions

Term	Acronym	Definition
Anonymisation		It is the process of either or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Business Continuity Plans	BCP	Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable defined level.
Caldicott Guardian	CG	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
CareCERT		NHS Digital has developed a Care Computer Emergency Response Team (**CareCERT**). CareCERT will offer advice and guidance to support health and social care

Term	Acronym	Definition
		organisations to respond effectively and safely to cyber security threats.
Code of Conduct		A set of rules to guide behaviour and decisions in a specified situation
Common Law		The law derived from decisions of the courts, rather than Acts of Parliament or other legislation.
Data 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 Processor		A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Act 1998	DPA 1998	An Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information
Data Protection Act 2018	DPA18	Act replaced DPA 1998 above and includes General Data Protection Regulations (GDPR)
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with GDPR requirements.
Data Protection Officer	DPO	A role with responsibility for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation
Data Security and Protection Toolkit	DSP Toolkit	From April 2018, the DSP Toolkit will replace the Information Governance (IG) Toolkit as the standard for cyber and data security for healthcare organisations
Data Sharing Agreement	DSA	A contract outlining the information that parties agree to share and the terms under which the sharing will take place.
Freedom of Information Act 2000	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities
Information Assets		Includes operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications
Information Commissioner's Office	ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by

Term	Acronym	Definition
		public bodies and data privacy for individuals.
Pseudonymisation		The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Senior Information Asset Owner	SIAO	Senior Information Asset Owners are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.
Senior Information Risk Owner	SIRO	Board member with overall responsibility for: • The Information Governance & Data Security and Protection Policies • Providing independent senior board-level accountability and assurance that information risks are addressed • Ensuring that information risks are treated as a priority for business outcomes • Playing a vital role in getting the institution to recognise the value of its information, enabling its optimal effective use.

4. Responsibility and Duties

4.1 Chief Executive

The Chief Executive has overall responsibility for ensuring that there are appropriate arrangements in place for the governing of all information processed within the Trust.

4.2 Data Protection Officer

- Under DPA18 the appointment of a Data Protection Officer is mandatory.
- The DPO provides the organisation independent risk-based advice to support its decision-making in the appropriateness of processing Personal and Special Categories of Data
- This includes UK General Data Protection Regulations (UK GDPR).
- The Data Protection Officer holds responsibility to the Chief Executive and Board with delegated roles and responsibilities documented in their job description.

4.3 Data Controller

Worcestershire Acute Hospitals NHS Trust is the Data Controller. The Chief Executive has

overall responsibilities for the organisation and may delegate relevant duties to both the Data Protection Officer and SIRO as appropriate.

4.4 Senor Information Risk Owner (SIRO)

- Chair the Information Governance Steering Group.
- Represent confidentiality and security issues at Trust Board level.
- Promoting a culture for protecting and using data
- Oversee the development of an Information Risk Policy.
- Take ownership of risk assessment process for information risk, including review of the annual information risk assessment.
- Review and agree actions in respect of identified information risks.
- Provides a focal point for managing and reporting information incidents
- Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately trained and briefed on information risk and data protection issues.
- Reporting the management of information risk directly to the Trust Management Executive (TME)

4.5 Caldicott Guardian

- Act as the 'conscience' of the Trust regarding confidentiality and ensure that the Trust satisfies the highest practical standards for the handling of patient information, both within the Trust and data flows to other NHS and non-NHS organisations.
- Ensure that there is a framework enabling Caldicott principles to be reflected in Trust's policies and procedures for the management and use of personal information.
- Be a member, and deputy chair, of the Information Governance Steering Group and participate in line with the terms of reference for that group.
- Supports the Information Governance Team in the development of information sharing protocols.
- Offer support and advice as required to the Information Governance Team on matters relating to confidentiality and patient information.
- Agree and review policies regarding the protection and use of personal information.
- Agree and review protocols governing the disclosure of personal information to partner organisations.
- Make the final decision on issues that arise regarding the protection and use of personal information.

4.6 Senior Information Asset Owner

- Understand the Trust's policies on the use of information and information risk management;
- Maintain an understanding of 'owned' assets and how they are used;
- Ensure that all Information Assets 'owned' are accurately recorded in the Master Asset & Applications Registry System (MAARS)
- Conduct quarterly risk assessment reviewed for all 'owned' information assets and ensure processes are in place to address these identified risks in line with the Trust's Information Risk Management Policy and relevant statutory and regulatory requirements;
- Ensure information training requirements are complied with; and

- Provide an annual written assessment to the SIRO for all 'owned' assets; and
- Give assurance to the SIRO that all aspects of this responsibility have been undertaken and that you are confident that your area complies with policy, regulations and the law.

4.7 Information Asset Owner/Administrator

All information assets recorded on MAARS will have a system owner. They will be assigned by the SIAO and will be responsible for the information contained within the system. The information asset administrator will manage the day to day running of the system.

4.8 Information Governance Manager

The Information Governance Manager is responsible for specialist information governance advice with a focus on national and local developments to enable compliance with Data Protection Act 2018 (General Data Protection Regulations 2016) and in addition, application of the Caldicott Principles and all aspects of confidentiality and data security.

The Information Governance Manager role is responsible for the successful delivery of the Data Security & Protection Toolkit and the agreed information governance framework for the Trust to meet its statutory obligations.

4.9 Head of Infrastructure and Cyber Security

The Head of Infrastructure and Cyber Security is responsible for ensuring that the Trust has a strategy in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials.

4.10 Managers

All managers are responsible for ensuring that their staff are adequately trained and conform to this policy

4.11 Employees, Contract and Agency Staff and Other People Working on Trust Premises

- All employees, including all staff seconded to the Trust, contract, voluntary, temporary and agency staff and other people working on Trust premises have a duty to comply with this policy. This includes members of staff with an honorary contract or paid an honorarium.
- Employees must ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that personal data is kept:
    - In a safe place where there would be no unauthorised access, and must not be left unattended in public/waiting areas
    - In a locked filing cabinet or drawer where possible
    - In an office with restricted access, or
    - On disk, memory stick or other electronic storage system, appropriate security measures must be used (contact the IT Service Desk for further information)
- Check that any personal data they provide to the Trust is accurate and up to date
- Ensure data provided by and recorded for others (i.e. patients) is accurate and up to date

- Inform the Trust of any changes to personal data they have provided, e.g. change of address, change of name, photographic identity
- Check the accuracy of data, including sensitive data, which the Trust may send out from time to time, in order to update existing personal data.
- Understand that they must be appropriately trained and supervised to handle data including requests for the disclosure or sharing of data

5. Policy detail

5.1 Registration and Notification to the Information Commissioner

The Information Governance Manager is responsible for notifying the Information Commissioner regarding the Trust's Data Protection Register Entry and for supplying details of any subsequent amendments.

5.2 Principles of the Data Protection Act 2018

- **Lawful, fair and transparent processing** – this principle emphasises transparency for all EU data subjects. When the data is collected, it must be clear as to why that data is being collected and how the data will be used.
- **Purpose limitation** – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place.
- **Data minimisation** – this principle instructs organisations to ensure the data they capture is adequate, relevant and limited.
- **Accurate and up-to-date processing** – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose.
- **Limitation of storage in the form that permits identification** – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached.
- **Integrity, Confidential and Secure** – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security).

General Data Protection Regulations (GDPR) also requires that:

- **Accountability and liability** – this principle ensures that organisations can demonstrate compliance.

5.3 Caldicott Guardian Principles

All NHS employees must be aware of the seven Caldicott Principles which apply to both patient and staff data.

Previous Caldicott reviews have made recommendations aimed at improving the way the NHS uses and protects confidential information.

- **Principle 1:** Justify the purpose - Why is the information needed
- **Principle 2:** Don't use patient identifiable information unless absolutely necessary – Can the task be carried out without identifiable information?

- **Principle 3:** Use the minimum necessary personal identifiable information – Can the task be carried out with less information?

- **Principle 4:** Access to patient identifiable information should be restricted to required/relevant personnel.

- **Principle 5:** Everyone with access to patient identifiable information should be aware of their responsibilities – *Lack of knowledge is not acceptable*

- **Principle 6:** Understand and comply with the law.

- **Principle 7:** The duty to share information can be as important as the duty to protect patient confidentiality

5.4 Individual Rights

Individuals legally have rights in relation to the data that is processed about them. The Trust must have processes in place should an individual choose to exercise any of their rights. It is vital that all staff can recognise such requests to allow them to be processed within the timescales set out in law.

- **The right to be informed**

The Trust has a privacy notice which is available through its public facing website. The purpose of the privacy notice is to inform the public about the collection and use of their personal data.

All Trust staff need to be aware of this notice and be able to direct individuals both to the notice and to where they can contact if they have any queries or concerns, usually the Data Protection Officer.

In addition to the privacy notice, the Trust will also provide individuals with more specific information at the time personal data is collected from them, for example when a complaint is made, or an individual signs up to be part of an engagement group. As it will vary as to when further information will need to be provided to individuals, the Information Governance Team should always be consulted to determine what is required in each circumstance.

- **The right of access**

Individuals, including staff, have the right to ask the Trust for confirmation of whether they process data about them, and if the Trust does, to have access to that data so the individual is aware and can verify the lawfulness of the processing.

- **The right to rectification**

If personal data that the Trust holds is found to be inaccurate or incomplete, individuals have the right to have it rectified. This includes any data that the Trust may have passed on to others, unless this proves impossible or involves disproportionate effort. If this is the case, the Trust will explain to the individual why this has not been possible.

- **The right to erasure**

The right to erasure is also known as 'the right to be forgotten' and means that individuals have the right to have personal data that the Trust holds about them erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- If the individual withdraws their consent for the Trust to process their data (if this was the basis on which it was collected).
- The personal data was unlawfully processed (i.e. a breach of UK data protection laws).
- The personal data has to be erased in order to comply with a legal obligation.

- **The right to restrict processing**

This right means that individuals have the right to 'block' or suppress processing of their personal data which means that if they exercise this right, the Trust can still store their data but not to further process it and will retain just enough information about the individual to ensure that the restriction is respected in future.

Individuals can ask us the Trust to restrict the processing of their personal data in the following circumstances:

- If they contest the accuracy of the data the Trust holds about them, the Trust will restrict the processing until the accuracy of the data has been verified;
- If the Trust is processing the individual's data as it is necessary for the performance of a public interest task and the individual has objected to the processing, the Trust will restrict processing while they consider whether their legitimate grounds for processing are overriding.;
- If the processing of the individual's personal data is found to be unlawful but they oppose erasure and request restriction instead; or
- If the Trust no longer needs the data held about the

- The right to data portability

The right to data portability allows the individual to obtain and reuse personal data they have provided to the Trust for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- **The right to object**

Where the Trust necessarily processes personal data for the performance of a task in the public interest/exercise of official authority, the individual has a right to object to the processing. They must have an objection on grounds relating to their particular situation.

If an individual raises an objection, the Trust will no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the individual's interests, rights and freedoms or the processing is for the establishment, exercise or defence of legal claims.

- **Rights in relation to automated decision making and profiling**

Automated individual decision-making is a decision made by automated means without any human involvement.

Examples of this include:

- an online decision to award a loan; and

- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Automated individual decision-making does not have to involve profiling, although it often will do.

- **The right to withdraw consent**

Although not specified as an individual right in GDPR, individuals do have the right to withdraw their consent for their data to be processed for any specified purpose. They can withdraw their consent at any time.

Where possible, the Trust will make sure that the individual is able to withdraw their consent using the same method as when they gave it.

If an individual withdraws their consent, the Trust must stop the processing of their data as soon as possible.

Further details of the rights of individuals and any requests made about their rights should be made to the Information Governance Team in the first instance.

5.5 Sensitive (Special Category) Personal Data

The Data Protection Act 2018 makes a distinction between personal data and "sensitive (Special Category)" personal data which refers to the following:-

- Racial or ethnic origin
- Ethnic Origin
- Politics
- Religious or other beliefs
- Trade Union membership
- Genetics
- Biometrics (where used for ID purposes)
- Physical or mental health or condition
- Sexual life or sexual orientation
- Criminal proceedings or convictions

Sensitive (Special Category) personal data can be processed provided that at least one of the following conditions has been met:-

- The Data Subject has given their explicit consent
- It is necessary for monitoring equal opportunities
- It is a legal requirement of the subject's employment
- It is necessary to protect the vital interests of the subject
- It is carried out by certain non-profit bodies established for political, philosophical, religious or trade union purposes
- It is necessary for legal proceedings
- It is necessary for medical purposes
- The Secretary of State has given consent
- It is necessary for the prevention or detection of any unlawful act
- It is necessary for the provision of services such as confidential counselling or advice
- It is necessary for insurance or occupational pension scheme contracts

This list is not exhaustive and new categories may be added by the Secretary of State.

5.6 Processing Data

An essential requirement of the DPA is that all data must be processed "fairly". The Trust will therefore ensure that:-

- The Data Subject will not be deceived or misled
- The Data Subject will be informed of the purpose for which the personal data is intended to be used by the Information Officer or their nominated deputy
- The Data Subject will be informed whether the data is likely to be passed to a third party

5.7 Transferring Data Abroad

Personal Data will not be transferred outside of the United Kingdom unless that country or territory "ensures adequate level of protection" for the rights and freedoms of Data Subjects.

Transfers of Data may take place:

- Where the data subject has given explicit consent
- It is necessary to perform or make a contract
- By reason of substantial public interest
- Is part of Personal Data on a Public Register
- Is on terms approved by the Information Commissioner
- Patient Identifiable Information must only be transferred outside the UK on approval of the Caldicott Group / Caldicott Guardian

6. Implementation of key document

6.1 Plan for implementation

The Information Governance Manager will ensure that this policy is available to all Divisional Managers within the Trust. It is then their responsibility to ensure that all staff groups within their area are directed to this policy.

Mandatory Data Security Awareness training covers the confidentiality of information and this is promoted within the trust on a regular basis.

6.2 Dissemination

This policy will be available on the Trust Intranet and a publication in the Trust Weekly Brief to inform staff of the update to the policy.

6.3 Training and awareness

All staff are mandated to complete Data Security Awareness training on an annual basis

7. Monitoring and compliance

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the Policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Section 4.4	Board is adequately briefed on all data protection issues	Standing agenda item on IGSG. Incident reporting	Monthly/Each IGSG	SIRO/IG Manager	Trust Management Executive/Trust Board	At least 4 times per year.
Section 4.4	Board receives dedicated regular Cyber specific training	Arranged via NHSD	Every 2/3 years	IG Manager	IGSG/TME/Trust Board	Annual DSPT submission

8. Policy review

This policy will be updated every two years by the Information Governance Manager and approved by the Information Governance Steering Group to reflect the Trust's development of policies and procedures and the changing needs of the NHS or when necessary following changes to the law.

9. References

The Data Protection Act 2018 (DPA18)
EU General Data Protection Regulations 2016 (now UK GDPR and included within DPA18)
Freedom of Information Act 2000
The Human Rights Act 1998
The Computer Misuse Act 1990
Caldicott Principals
NHS Data Security and Protection Toolkit
Data Protection Good Practice – Information Commissioners Office
NHS Employers – Policies and best practice procedures
Benchmarking other NHS and Public Sector Data Protection practices
Information Governance Policy
Confidentiality Code of Conduct Policy
Corporate Records Management Policy
Health Records Management Policy
IT Security Policies

10. Background

10.1 Equality requirements

No impact from the equality assessment (Supporting Document 1)

10.2 Financial Risk Assessment

No impact from the financial risk assessment (Supporting Document 2)

10.3 Consultation Process

The policy has been created by the Information Governance Manager with input from the Information Governance Steering Group. The original policy was also been reviewed by the Policy Working Group.

10.4 Approval Process

This policy will be approved at the Information Governance Steering Group and sent on the Joint Negotiating and Consultation Committee (JNCC) for information.

Contribution List
This key document has been circulated to the following individuals for consultation;

Designation
Members of the Information Governance Steering Group, who include: SIRO, DPO, Caldicott Guardians, SIAO

This key document has been circulated to the chair(s) of the following committee's / groups for comments;

Committee
Information Governance Steering Group members

10.5 Version Control

Date	Author	Version	Page	Reason for Change
Sept 2021	IG Manager	1	All	Total re-write to align all Information Governance policies

Supporting Document 1- Equality Impact Assessment Tool

NHS Worcestershire Acute Hospitals NHS Trust

Herefordshire & Worcestershire STP - Equality Impact Assessment (EIA) Form
Please read EIA guidelines when completing this form

Section 1 - Name of Organisation (please tick)

Herefordshire & Worcestershire STP		Herefordshire Council		Herefordshire CCG	
Worcestershire Acute Hospitals NHS Trust	X	Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health and Care NHS Trust		Wye Valley NHS Trust		Other (please state)	

Name of Lead for Activity	**Senior Information Risk Owner**

Details of individuals completing this assessment	**Name**	**Job title**	**e-mail contact**
	Annie Osborne-Wylde	**IG Manager**	**Annie.osborne-wylde@nhs.net**
Date assessment completed	**20th September 2021**		

Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	**Title:** Data Protection Policy			
What is the aim, purpose and/or intended outcomes of this Activity?	Policy document to inform all staff.			
Who will be affected by the development & implementation of this activity?	❑ Service User ❑ Patient ❑ Carers ❑ Visitors		x Staff ❑ Communities ❑ Other _____	
Is this:	❑ Review of an existing activity X New activity			

	❑ Planning to withdraw or reduce a service, activity or presence?
What information and evidence have you reviewed to help inform this assessment? (Please name sources, eg demographic information for patients / services / staff groups affected, complaints etc.	New policy following total review of all IG policies
Summary of engagement or consultation undertaken (e.g. who and how have you engaged with, or why do you believe this is not required)	WAHT Information Governance Steering Group
Summary of relevant findings	Approved

Section 3

Please consider the potential impact of this activity (during development & implementation) on each of the equality groups outlined below. **Please tick one or more impact box below for each Equality Group and explain your rationale**. Please note it is possible for the potential impact to be both positive and negative within the same equality group and this should be recorded. Remember to consider the impact on e.g. staff, public, patients, carers etc. in these equality groups.

Equality Group	Potential positive impact	Potential neutral impact	Potential negative impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Age		X		
Disability		X		
Gender Reassignment		X		
Marriage & Civil Partnerships		X		
Pregnancy & Maternity		X		
Race including Traveling Communities		X		
Religion & Belief		X		
Sex		X		
Sexual Orientation		X		

Equality Group	Potential positive impact	Potential neutral impact	Potential negative impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Other Vulnerable and Disadvantaged Groups (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling **Other Vulnerable and Disadvantaged Groups** (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)		X		
Health Inequalities (any preventable, unfair & unjust differences in health status between groups, populations or individuals that arise from the unequal distribution of social, environmental & economic conditions within societies)		X		

Section 4

What actions will you take to mitigate any potential negative impacts?	Risk identified	Actions required to reduce / eliminate negative impact	Who will lead on the action?	Timeframe
How will you monitor these actions?				
When will you review this EIA? (e.g in a service redesign, this EIA should be revisited regularly throughout the design & implementation)				

Section 5 - Please read and agree to the following Equality Statement

1. Equality Statement

1.1. All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess and consult on how their policies and functions impact on the 9 protected

characteristics: Age; Disability; Gender Reassignment; Marriage & Civil Partnership; Pregnancy & Maternity; Race; Religion & Belief; Sex; Sexual Orientation

1.2. Our Organisations will challenge discrimination, promote equality, respect human rights, and aims to design and implement services, policies and measures that meet the diverse needs of our service, and population, ensuring that none are placed at a disadvantage over others.

1.3. All staff are expected to deliver services and provide services and care in a manner which respects the individuality of service users, patients, carer's etc, and as such treat them and members of the workforce respectfully, paying due regard to the 9 protected characteristics.

Signature of person completing EIA	
Date signed	
Comments:	
Signature of person the Leader Person for this activity	
Date signed	
Comments:	

Supporting Document 2 Financial Risk Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	None

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval