Information Governance Policy

Department/ Service:	Information Governance
Originator:	Head of Digital Governance and Compliance
Accountable Director:	Chief Digital Information Officer (Senior Information Risk Owner – SIRO)
Approved by:	Information Governance Steering Group (IGSG)
Date of approval:	4th June 2025
Revision due: **This is the most current document and should be used until a revised version is in place**	4th June 2028
Target Organisation(s):	Worcestershire Acute Hospitals NHS Trust
Target Departments:	All departments
Target Staff Categories:	All Trust staff/contractors/volunteers

Policy Overview:
This policy covers how and why information is managed and protected in the Trust. The structure of authority around the Trust's information, who owns it and how we are all responsible for safeguarding it.

Key Amendments to this Document

Date	Amendment	Approved by:
4th June 2025	Updated following review of the Data Security and Protection Toolkit	IGSG
July 2024	Document extended for 6 months whilst documents are reviewed in line with new Data Security and Protection toolkit	
September 2021	Total re-write to align all Information Governance policies	
March 2021	Document extended for 6 months as per Trust agreement	
Dec 2020	Document extended for 3 months until March 2021 due to urgent COVID work	Rebecca Brown

Contents page:

1. Introduction

The aim of this policy is to provide the employees of Worcestershire Acute Hospitals NHS Trust with a simple framework through which the elements of Information Governance (IG) will be met.

Information is the most important asset available to an organisation and therefore all organisations must have robust arrangements for Information Governance (IG) which are reviewed annually and described in the Data Security and Protection Toolkit (DSPT).

Information Governance is owned by the Trusts most senior management, and this is demonstrated by signing annually a Statement of Compliance via the Data Security and Protection Toolkit (DSPT) in respect to the Trust and any contracted services.

IG compliance is also supported by the identification of Senior Information Asset Owners, Information Asset Owners/Administrators, Data Mapping and Information Asset Registers through a process of risk management.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient, and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

This policy includes the approach to the security and governance of information, systems and networks supporting the operation of essential function(s)

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.

The policy covers all aspects of information within the organisation, which support the Trust Essential Functions, including:

- Patient information

- Staff information
- Organisational information

3. Definitions

Definition	Description
Caldicott Guardian (CG)	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
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 (DPA98)	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 (DSPT)	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 Processing Agreement (DSPA)	A contract outlining the information that parties agree to share and the terms under which the sharing will take place.
Essential Functions	Essential functions are all the parts of the organisation that are necessary to deliver WAHT services.
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 public bodies and data privacy for individuals.
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. Trust Board Responsibility

It is the role of the Trust Board to define the organisation's policy in respect of Information Governance, considering legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

4.2. Trust 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.

4.3. Data Protection Officer (DPO)

- 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 Trust Board with delegated roles and responsibilities documented in their job description.
- They are responsible for ensuring the Information Commissions Data Protection Registry is reviewed annually and updated where appropriate.
- The DPO is responsible for ensuring that this policy is updated following any changes in law or requirements following major incidents or data breaches

4.4. 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.

4.5. Senior 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
- Take ownership of risk assessment process for information risk
- 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 Board (TMB)

4.6. Caldicott Guardian (CG)

- 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.

4.7. Senior Information Asset Owner (SIAO)

- 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.

4.8. 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.

4.9. Data Governance and Compliance Manager

- The Data Governance and Compliance Manager is responsible for specialist data protection and 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.
- They are responsible for the management of the Data Security & Protection Toolkit (DSPT) and the agreed information governance framework for the Trust to meet its statutory obligations.
- They will ensure that the contents of this policy is communicated to staff on a regular basis, both as whole policy or guidance/articles relating to it. This communication will include relevant senior managers and governance teams.

4.10. Chief Technology Officer

- The Chief Technology Officer 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.

4.11. Managers

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

4.12. 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

The following areas are all parts of Information Governance/Data Protection and underpin confidentiality principle

5.1. National Data Security Standards/CAF Aligned Data Security and Protection Toolkit (DSPT)

Since 2018, the DSPT has used the National Data Guardian's 10 data security standards as the measure against which organisations must assess their data protection and security capability and preparedness. However, the National Data Guardian standards will gradually be phased out as the basis of the DSPT's assessment and replaced by the National Cyber Security Centre's Cyber Assessment Framework (CAF).

The CAF was adopted as the new basis for DSPT assurance, when published in September 2024

The CAF Aligned DSPT now has 5 objectives:

- A: Managing Risk
- B: Protecting against cyber-attack and data breaches
- C: Detecting cyber security events
- D: Minimising the impact of incidents
- E: Using and sharing information appropriately

5.2. Openness

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

Information will be defined and where appropriate kept confidential, underpinning the Caldicott Principles and the regulations outlined in the Data Protection Act 2018.

Non-confidential information on the Trust and its services will be available to the public through a variety of media, including its internet-based Publication Scheme, in line with the Trust's code of openness.

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

Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.

The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

The Trust will have clear procedures and arrangements for handling queries from patients and the public regarding the information handling and processing activities being undertaken by the organisation.

Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

Data Security Awareness (DSA) annual training including awareness and understanding of the National Data Guardian (Caldicott) principles, confidentiality, information security and data protection will be mandatory for all staff.

5.3. Legal Compliance

The Trust regards all identifiable personal information relating to patients as confidential, including information pertaining to deceased patients.

The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.

The Trust regards all identifiable personal information relating to current and ex-staff members as confidential except where national policy on accountability and openness requires otherwise.

The Trust will establish and maintain policies to ensure compliance with the:

- UK Data Protection Act 2018
- General Data Protection Regulations
- Freedom of Information Act 2000
- Human Rights Act 1998
- Common Law Duty of Confidentiality

The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation, including:

- Health & Social Care (Quality & Safety) Act 2015
- Health & Social Care Act 2012
- Crime and Disorder Act 1998
- Protection of Children Act

The Trust is bound by the provisions of a number of laws and regulations. The list below is not exhaustive, and other legislation and regulations may also apply.
Laws:

- National health Service Act 1977 / 2006
- Environmental Information Regulations 2004
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Crime and Disorder Act 1998
- Road Traffic Act 1988
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998
- Public Records Act 1958, 1967 and 2005

Regulations:

- Caldicott Committee Report 2013
- Records Management: Code of Practice 2021
- Care Quality Commission Standards

The Trust is registered with the Information Commissioners Office as a Data Controller and processor of information and must comply with its duties as defined by this registration.

The aim of this policy and management framework is to ensure compliance with the strategic objectives and legal obligations above and DSPT requirements. A schedule of DSPT

compliance is an integral part of the action plan which is regularly reviewed and updated at the Information Governance Steering Group (IGSG).

5.4. Information Security

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

In the event of the transfer of personal information to countries outside of the UK, this will be undertaken in accordance with the Data Protection Act 2018 and Department of Health guidelines.

The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.

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

The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

5.5. Information Quality Assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.

Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

Wherever possible, information quality should be assured at the point of collection.
Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

The Trust will promote information quality and effective records management through policies, procedures / user manuals and training.

5.6. Information Governance Steering Group

The Information Governance Group (IGSG) is accountable to the Trust Management Executive (TME) and has responsibility to ensure the Trust adheres to the Information Governance Policy. There are three subgroups which report into IGSG; Data Quality Steering Group; Information Security Risk Forum and the Health Records Group.

The IGSG agenda is structure to monitor compliance with the National Data Security Standards and sign off completion of the NHS Digital Data Security and Protection Toolkit.

The purpose and functions of the IGSG are set out in the IGSG Terms of Reference. The terms of reference are updated annually. For further information contact the Information Governance team.

5.7. Reporting for Information and Cyber related incidents

Failure to comply with this policy may result in breaching the GDPR/Data Protection Act (and other legal and regulatory) requirements, resulting in a fine from the Information Commissioner. Where there is a breach of confidentiality or loss of data or information asset, this must be reported and managed via the incident reporting process (via the incident reporting system Datix). If the incident has an adverse impact on the Trusts essential services or functions, these will be managed appropriately.

All serious incidents are assessed for possible external reporting and reported on NHS Digital Incident Reporting Tool on the DSPT within 72 hours of the start of the incident. This will automatically result in a referral to the Information Commissioner's Office.

Any potential Level 2 incident will be assessed using the Trusts serious incident reporting process managed by the Information Governance team. Once this is completed, and the severity is confirmed, the Data Protection Team will then inform the Assistant Director of Information and performance, SIRO, Data Protection Officer and Caldicott Guardian for approval to report the incident externally.

The Data Governance and Compliance Manager will work with the Information Commissioners Officer investigators to provide and further information that may be required.

5.8. Learning from incidents

The Information Governance Steering Group will receive regular reports of incidents; analysis of trends and review copies of Incident Management Reports to ensure the mitigation of the risk and share learning across the Trust.

Following a major Data Protection incident or data breach, learning will be presented to the IGSG and incorporated into updated processes or guidance. This may include process implementation steps, mitigations and defines actions.

This will ensure that polices and processes are adapted to incorporate any improvements required.

It is noted that in some cases, incidents may involve staff members, and any investigations will be aligned to the relevant Human Resources policies and procedures.

5.9. Data Protection knowledge validation

The Trust will have an audit plan in place to ensure that staff are aware of their responsibilities around Data Protection. This will ensure that there is validation in place (spot checks and surveys) where staff knowledge is tested and validated.

5.10. Training Requirements

All new staff will receive information on the requirement to complete Data Security Awareness training on Induction. Data Security training is mandatory and must be completed using the online Data Security Awareness training accessed in ESR. Some specific ancillary staff may complete the same training using a paper version which is sent to the Information Governance team to be inputted manually into ESR.

Annual mandatory on-line Data Security Awareness training is mandatory for all employed staff (both permanent and temporary).

In addition, some roles are required to complete additional training, (e.g. the Data Protection Officer; SIRO, Caldicott Guardian, IT Security Specialist)

The Board are required to receive risk management training.

Compliance with the mandatory annual training is monitored by the Data Protection team and there is an escalation process for non-compliance.

5.11. Data Protection Impact Assessments (DPIA)

All staff should be aware of the relevant procedures applicable when implementing any change to the way the Trust collates, processes or shares information. Staff should be aware that there can be no change to service delivery without appropriate Information Governance sign off.

A Data Protection Impact Assessment is required when a proposed change to service delivery involves the way the Trust collates, processes or shares information.

The ICO recommends all organisations whose practices and technology create a high level of risk to the privacy rights of its data subjects. Organisations must be able to demonstrate that a DPIA has been carried out, or penalties can be enforced against the organisation.

There is a template used for the completion of a DPIA and guidance may be obtained from the Information Governance Team.

All DPIAs are signed off by the Caldicott Guardian (patient data) or the SIRO (staff data), assessed for information security issues and will be noted at the IGSG.

5.12. Data Sharing/Processing Agreements

If a DPIA shows a process or system where data will be shared and may have an impact on the privacy of individuals, it will be necessary for a sharing agreement to be put in place. These may be called data or information, sharing or processing, agreements or protocols. The Trusts DPIA process refers to them as Data Sharing/Processing Agreements (DSPA).

The Data Sharing Processing Agreements will be approved by the same process as the DPIAs.

5.13. Advice and Guidance relating to Information Governance/Data Protection

This policy sets out the overarching Information Governance principles and the Head of Digital Governance and Compliance/DPO will ensure that advice and guidance documentation is available on related topics, and they will be regularly included in communication messages to staff.

Guides are available on the following webpage

6. Implementation

6.1. Plan for Implementation

The Data Governance and Compliance Manager will ensure that this policy is available to all staff within the Trust.

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

6.2. Dissemination

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

A link to this policy will be placed on the Data Protection Webpages

6.3. Training and Awareness

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

7. Monitoring and Compliance

Section / page no:	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 the check reported to:	Frequency of reporting:
No.	**WHAT?**	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Section 4.1	Reporting the management of information governance framework to the Trust Management Executive (TME)	Standing agenda items on IGSG agenda	Each IGSG meeting	Head of Digital Governance and Compliance	Trust Management Executive	4 times a year
Section 5.1	DSPT compliance monitored via actions plans and annual submission	Actions plans monitored at IGSG meetings and submission in line with NHSD requirement.	Each IGSG meeting	Head of Digital Governance and Compliance	IGSG / TME	4 times a year
Section 5.8	Compliance with Mandatory Annual Data Security Awareness Training	Monthly training dashboard	Monthly	Head of Digital Governance and Compliance	IGSG	4 times a year
Section 5.7	Serious Incident reporting	Reported on Datix and externally to ICO on condition of meeting the criteria	IGSG	SIRO/ Head of Digital Governance and Compliance	IGSG / TME	4 times a year

8. Policy Review

This policy will be updated every three years by the Data Governance and Compliance 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
- WAHT Code of Conduct in Respect of Confidentiality
- WAHT Corporate Records Management Policy
- WAHT ICT Policy
- WAHT Data Protection Policy

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

The policy has been created by the Data Governance and Compliance Manager with input from the Information Governance Steering Group.

Contribution List This key document has been circulated to the following individuals for consultation:	
Name	**Designation**
See below	
This key document has been circulated to the chair(s) of the following committees / groups for comments:	
Information Governance Steering Group (IGSG), Membership includes: SIRO, DPO, Caldicott Guardian, SIAO	

10.4. Approval Process

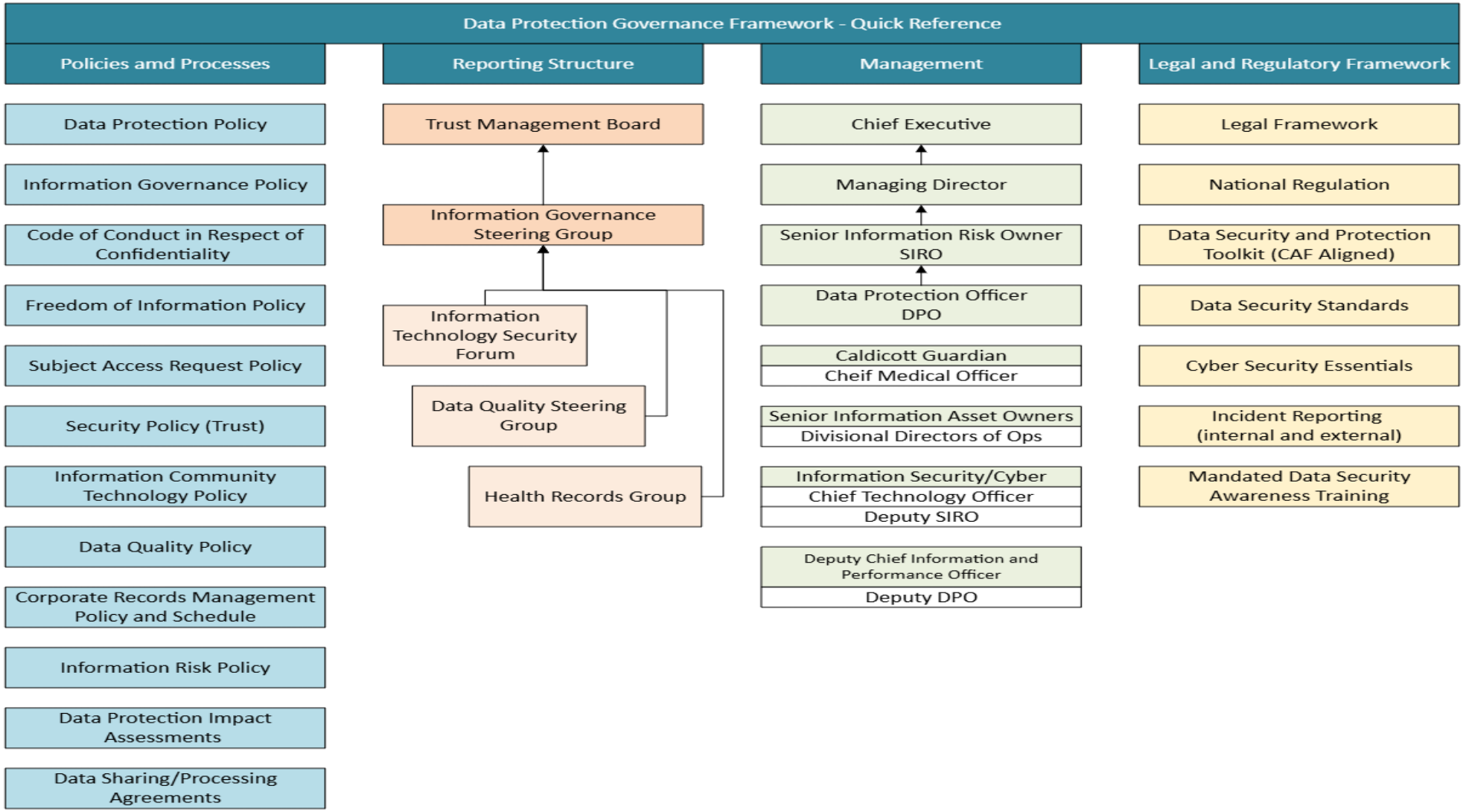
This policy will be approved at the Information Governance Steering Group and ratified at the Trust Management Board (TMB)

10.5. Version Control

Date	Amendment	Approved by:
	Updated reporting structure and approval process	IGSG
	Updated Caldicott Function appendix	IGSG
	Updated reference section with updated trust policies	IGSG
	Updated PCD appendix and reference to PID throughout policy	IGSG
06 March 2020	Remediation of policy suite on behalf of the Trust.	IGSG
Sep 2021	Re-write	IGSG
June 2025	Update in line with review timescale	IGSG

11. Appendices

Appendix 1 – Data Protection Governance Framework - Quick Reference



12. Supporting Document 1 – Equality Impact Assessment Form

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

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	✓	Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health and Care NHS Trust		Wye Valley NHS Trust		Other (please state)	

Name of Lead for Activity	

Details of individuals completing this assessment	**Name**	**Job title**	**e-mail contact**
	Matthew Thurland	**Head of Digital Governance and Compliance**	**Wah-tr.dataprotection@nhs.net**
Date assessment completed			

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 staff of Data Protection framework

Who will be affected by the development & implementation of this activity?	❑ ❑ ❑ ❑	Service User Patient Carers Visitors	☒ ❑ ❑ ❑	Staff Communities Other _____
Is this:	☒ Review of an existing activity ❑ 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.	This policy is regulated by Data Protection Law			
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		

Equality Group	Potential positive impact	Potential neutral impact	Potential negative impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Sexual Orientation		x		
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:	

13. Supporting Document 2 – Financial Impact Assessment

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

ID	Financial Impact:	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		