The Royal Wolverhampton NHS
NHS Trust

OP13 v8.2

Information Governance & Data Protection Policy

Contents

Policy Sections **Page**

1.1 Policy Statement 2
1.2 Definitions 3
1.3 Accountabilities 6
1.4 Policy Detail 11
1.5 Financial Risk Assessment 11
1.6 Equality Impact Assessment 11
1.7 Maintenance 11
1.8 Communication and Training 11
1.9 Monitoring Process 12
1.10 Auditing 12
1.11 References 13
1.12 Strategies 15
1.13 Other Sources 15

Procedures

Procedure 1 Data Protection Procedure
Procedure 2 Data Protection Impact Assessment (DPIA) Procedure
Procedure 3 IG/ Data Security Incidents Procedure
Procedure 4 Information Asset Management and Procedure
Procedure 5 National Data Opt Out Procedure

Supporting Attachments

Attachment 1 Application of Data Protection Principles
Attachment 2 Breakdown of the NHS statutory lawful bases for processing data
Attachment 3 Consent Form Examples
Attachment 4 Privacy Notice Template
Attachment 5 Data protection Impact Assessment Template
Attachment 6 IG/ Data Security Incidents -Root Cause Analysis Template
Attachment 7 IG Audit Templates
Attachment 8 Template for Notification to individuals regarding an incident.

1 Information Governance/ Data Protection Policy

1.1 Policy Statement: Information Governance (IG)/ General Data Protection Regulation (GDPR)

This policy sets out the approach that The Royal Wolverhampton NHS Trust (RWT) will take to establish and maintain a robust Information Governance (IG) framework, ensuring that all information is handled legally, securely, ethically, and effectively.

The policy brings together the statutory requirements, NHS obligations, and recognised best practice that apply to the creation, use, sharing, retention, and disposal of information held by the Trust. This policy defines the Trust's legal framework for compliance with:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018
- the Data (Use and Access) Act 2025 (DUAA)

These legislative frameworks must be interpreted collectively to ensure that the Trust meets its legal responsibilities and upholds the rights of data subjects. Information is a vital asset to the Trust, both for the safe and effective care of patients and for the efficient management of services, resources, and corporate functions. It is therefore essential that all information is accurate, appropriately accessible, protected against unauthorised access or loss, and used in a manner that fosters public trust and confidence.

Information Governance provides the framework through which the Trust and its workforce ensure that information is:

- processed lawfully, fairly, and transparently
- accurate and kept up to date
- stored securely and protected from unauthorised access, loss, or misuse
- retained and disposed of in line with legal and business requirements

This policy applies to all information processed by the Trust, in any format, and to all individuals working on behalf of the Trust, including employees, temporary staff, contractors, students, and volunteers, as defined in section 1.3.5.

Specifically, this policy:

- sets out the Trust's overarching approach to the protection and use of information
- defines roles and responsibilities for those within the scope of the policy
- details procedures and attachments that provide purpose-specific guidance

Compliance with this policy is mandatory. Failure to do so may result in disciplinary action and could expose the Trust and individuals to regulatory or legal sanctions.

1.2 Definitions

Anonymised Data -Data that has been processed so that individuals can no longer be identified, either directly or indirectly. Fully anonymised data is not classed as personal data under data protection legislation.

Controller (Data Controller) - A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data.

Corporate Information -Information used in the Trust's business and administrative functions, including but not limited to policies, procedures, minutes, agendas, financial records, and committee or meeting papers.

Criminal Offence Data - Personal data relating to the commission or alleged commission of an offence, criminal convictions, criminal proceedings, their disposal, or sentencing. This data is subject to specific safeguards under the Data Protection Act 2018.

Data Protection Act 2018 (DPA) - UK legislation that supplements and enacts the UK General Data Protection Regulation into domestic law.

Data Protection Legislation -All applicable laws and regulations relating to the processing of personal data and privacy, including:

- Data Protection Act 2018
- UK GDPR
- Data (Use and Access) Act 2025
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Electronic Communications Data Protection Directive 2002/58/EC
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

Data Subject- A living, identifiable individual to whom personal data relates, including (but not limited to) a member of staff, patient, service user, or member of the public.

DSPT – Data Security and Protection Toolkit - The NHS England online self-assessment tool used to measure and evidence organisational compliance with data protection, information governance, and cyber security standards. Completion is mandatory for organisations that access NHS patient data.

DUAA – Data (Use and Access) Act 2025 -UK legislation providing a statutory framework for the lawful use, sharing, and access to data, including personal data, while maintaining appropriate safeguards for privacy and security.

EEA State - A country that is a member of the European Economic Area (EEA).

GDPR / UK GDPR – General Data Protection Regulation - The retained UK version of Regulation (EU) 2016/679 governing the processing of personal data, applied alongside the Data Protection Act 2018.

IAA – Information Asset Administrator- An individual responsible for the day-to-day management of information assets on behalf of the Information Asset Owner. Further details are set out in the Accountability section.

IAO – Information Asset Owner -A senior individual with responsibility for understanding, managing, and mitigating risks associated with one or more information assets. Further details are set out in the Accountability section.

IAMG – Information Asset Management Group - A group responsible for oversight and assurance of information asset management across the Trust.

IG – Information Governance -The framework of policies, procedures, roles, and controls that ensure information is managed lawfully, securely, efficiently, and ethically throughout its lifecycle.

IGAG – Information Governance Action Group -The group responsible for coordinating, monitoring, and delivering Information Governance actions and compliance activity.

IGSG – Information Governance Steering Group - The senior group with the delegated responsibility to provide strategic oversight and assurance for Information Governance arrangements.

Personal Data / Personal Information - Any information relating to a living, identifiable individual, including patients, staff, or members of the public. An individual may be identified directly or indirectly, for example by name, identification number, NHS number, date of birth, address, Internet Protocol (IP) address, or other factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Processing - Any operation or set of operations performed on personal data, whether automated or not, including obtaining, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, aligning or combining, restricting, erasing, or destroying data.

Processor (Data Processor) - A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.

Pseudonymised Data - Personal data in which identifiers have been replaced with a pseudonym, so individuals cannot be identified without the use of

additional information, which is kept separately and securely. Pseudonymised data remains personal data under data protection legislation.

Special Category Data (Sensitive Personal Data) - Personal data revealing or concerning the following categories, which are subject to enhanced protection:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health conditions
- Genetic data
- Biometric data (where used for identification)
- Sexual life or sexual orientation

1.3 Information Governance and Data Protection and Security Accountabilities

1.3.1 Obligations of the Organisation

The Organisation will, through appropriate management oversight and the application of robust criteria and controls:

- Ensure that personal data is processed fairly, lawfully, and transparently, and that the conditions for the collection and use of information are fully observed.
- Meet its legal obligations to clearly specify and document the purposes for which personal data is collected and used.
- Collect and process only such information as is necessary, relevant, and proportionate to fulfil operational requirements or to comply with statutory and regulatory obligations.
- Maintain the accuracy and quality of information, including through appropriate validation and verification processes with patients, staff, or relevant individuals.
- Apply defined retention and disposal controls to ensure information is held only for as long as necessary, in accordance with approved retention schedules.
- Ensure that the rights of individuals (data subjects) whose information is held can be fully exercised in accordance with Data Protection Legislation
- Take appropriate technical and organisaional security measures to protect personal information against unauthorised or unlawful processing, loss, destruction, or damage.
- Ensure that personal data is not transferred outside the UK or European Economic Area (EEA) unless appropriate safeguards and lawful transfer mechanisms are in place.
- Promote and uphold the ethical use of data, ensuring information is used in ways that are fair, proportionate, transparent, and consistent with individuals' reasonable expectations, professional standards, and organisaional values.

1.3.2 Senior Accountabilities

Chief Executive Officer is the accountable officer for the Trust.

Data Protection Officer (DPO) the Trust is the Head of Data Security and Protection. The DPO is responsible for informing and advising the Trust, its processors, and its employees of their obligations under the General Data Protection Regulation (UK GDPR) and other applicable Data Protection Legislation. The DPO will:

- Act independently in the performance of their duties
- Monitor and advise on compliance with data protection legislation, policies, and procedures

- Provide guidance on data protection requirements, including privacy by design, data protection impact assessments, and data subject rights
- Act as a point of contact for the Information Commissioner's Office (ICO) and cooperate with the supervisory authority as required
- Have access to all information, systems, processing activities, and personnel necessary to perform their role effectively

The DPO will carry out their duties without receiving instructions regarding the exercise of their data protection tasks and will report at an appropriate senior level to ensure independence, authority, and effectiveness.

Chief Medical Officer is the appointed ***Caldicott Guardian*** for the Trust and has, on behalf of the Board, responsibility to act as the Guardian of patient identifiable information and chair of the Information Governance Steering Group (IGSG)

Chief Financial Officer is the ***Senior Information Risk Officer*** (SIRO) who acts as an advocate for information risk on the Board and understands how the strategic business goals of the Trust may be impacted by information risks.

Caldicott and SIRO responsibilities are:

The Caldicott Guardian and Senior Information Risk Owner (SIRO) are responsible for providing strategic leadership and oversight of information risk management within the Organisation. Their responsibilities include:

- Overseeing the development, implementation, and ongoing review of the Information Risk Policy and associated strategy within the wider Information Governance Framework
- Taking ownership of the information risk assessment process, including the review of the annual information risk assessment to support and inform the Statement of Internal Control / Annual Governance Statement
- Reviewing identified information risks and agreeing appropriate actions, mitigations, and risk acceptance decisions
- Ensuring that the Organisation's approach to managing information risk is effective, proportionate, and adequately resourced, and that expectations and responsibilities are clearly communicated to all staff
- Acting as a focal point for the identification, escalation, discussion, and resolution of information risk and information-sharing issues
- Ensuring that the Board is appropriately briefed and assured on information risk matters, including significant incidents, emerging risks, and compliance with Data Protection and Information Governance requirements

Each Senior Manager: Responsible for ensuring that the personal data held by their department is kept securely and used properly, within the terms of the Act. They are also responsible for informing Trust of the types of personal data held in their directorate, and any changes or new holdings to inform the Information Commissioner as required.

1.3.3 Board, Committee and Groups

Trust Board Will receive risk and assurance report which will include the approval of the annual DSP Toolkit return.

Quality and Safety Oversight Group (QSOG) will monitor compliance with the DSP Toolkit standards by receiving 2 times yearly reports in line with the 2 yearly DSP Toolkit submissions to NHS England. Risks, incidents and exceptions to compliance status will be reported to this group.

Information Governance Steering Group (IGSG) The Caldicott Guardian chairs the IGSG. The group has specific terms of reference, and its membership includes representatives from the divisions within the Trust as well as DSP Toolkit objective leads. The IG Steering Group (IGSG) has overall responsibility for overseeing the development and implementation of IG strategy, Policy and action plans. These will be subject to a periodic review and progress reports to the Compliance Committee, Board Assurance Committee, Trust Management Team and Trust Board.

Information Governance Action Group (IGAG) will monitor actions arising from the IGSG and ensure continued improvement for the DSP Toolkit and any other Information Governance Action Plans, which is fed back to the Information Governance Steering Group.

Data Privacy Impact Assessment Group (DPIA Group) has delegated responsibility from IGSG to review assurances around DPIA assessment and to ensure data protection by design measures are adequately assessed.

The Information Asset Management Group (IAMG) - chaired by the Senior Information Risk Owner (SIRO), operates under delegated authority from the Information Governance Steering Group (IGSG) to provide oversight and assurance that information assets are effectively identified, mapped, and risk assessed across the organisation. The IAMG will also monitor compliance, escalate risks where appropriate, and provide assurance to the IGSG on the effectiveness of information asset management arrangements.

The Data Ethics Group (DEG), acting under delegated authority from the Information Governance Steering Group (IGSG), is responsible for providing oversight and assurance that all uses of patient and other identifiable data are conducted in an ethical, lawful, and transparent manner. The DEG will also promote best practice in ethical data use and provide advice and recommendations to support compliant decision-making across the organisation.

1.3.4 Specialist Staff

Information Governance Manager is responsible for coordinating Information Governance improvement activities, providing advice and guidance across the Trust.

Group Head of Cyber Securityis responsible for coordinating information security activities, providing advice and assistance across the Trust. Continuously assessing the shortfall between security measures in place being effective and those established at a policy level thus highlighting deficiencies for remedial action. Investigating suspected and actual breaches of security and undertaking reporting/remedial action as required to IGAG.

Information Governance Team are responsible for overseeing and supporting the use of information across the trust. The team ensures that information is handled in accordance with legal, regulatory and the organisations requirements.

Objective leads for DSPT are responsible for monitoring/maintaining evidence and identifying risks associated with the respective standard that falls within the scope of their role and for embedding any the standards across the Trust.

Information Asset Owners (IAO) will be the nominated owner(s) for one or more identified information assets they have clear responsibility to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities in relation to information security and risks associated with the asset.

Information Asset Administrators (IAA) have responsibility for the day-to-day management of information assets, ensure that policies and procedures around the asset are followed, and to consult their IAO on potential or actual security incidents and risks.

Health Records Access Team will respond to Subject Access Requests from the public regarding health records and the **HR Department** will handle subject access requests from staff regarding personnel matters whether current or past employees. Both will keep logs of requests made and ensure a formal response is provided to the requester, either by way of providing the information or else by advising them of the reasons why the information will not be made available. They will ensure that the relevant time scales for responses, outlined in the law, are complied with, and compliance is reported to an overseeing group, or the Information Governance Steering Group.

1.3.5 All Staff

Managers throughout all levels of the organisation (i.e. Team Leaders, Supervisors, Matrons, Clinical Directors) have a responsibility for implementing all elements of Information Governance and providing, or accessing, appropriate levels of expertise.

The Trust and all its employees, whether they are on permanent, fixed term or temporary contracts, contractors, students and voluntary; have a legal obligation and a duty of confidence to ensure that any information processed is done so in line with legal requirements and best practice.

All Staff will ensure that they have read this Policy and have undertaken the relevant mandatory training in Information Governance in line with the Trusts Induction and Mandatory Training Policy OP41.

It remains the responsibility of all staff members to adhere to all relevant Organisational policies and procedures, and also current law and legislation, when dealing with personal or sensitive information during the course of their duties, in particular the Data Protection Act 2018, the Common Law Duty of Confidentiality and the Caldicott Principles.

All staff must check that whatever information they provide in connection with their own employment is accurate and up to date and that they have a responsibility for informing relevant departments of any errors or changes required to that information.

All staff are encouraged to report untoward incidents and identify risks, no matter how minor they appear, this would not only apply to clinical incidents but also to information security breaches, following Procedure 4- Data Security and Protection Incidents Procedure. Staff can also refer to the Department of Health guidance: NHS information Governance – guidance on legal and professional obligations

1.3.6 3rd Parties

Any 3rd party with access to Trust data or processing Trust data is also bound by the Data Protection Act 2018.

The specific responsibilities for Data Controller and Data Processors will be described in the 3rd parties' contract with the Trust including any extra confidentiality or non-disclosure statements where they are needed. 3rd parties must abide by the terms of their contract.

1.4 Policy Detail

There are five key interlinked strands to the Information Governance Policy:

1. The proactive use of information
2. Openness and confidentiality
3. Legal compliance
4. Information security
5. Information quality assurance

RWT has developed several related policies and procedures to cover all aspects of Information Governance which are aligned with the Data Security and Protection Toolkit requirements and relevant Data Protection law. The key Data Protection policy detail can be found in Procedure 1.

1.5 Financial Risk Assessment

A financial risk assessment has been undertaken, and no financial risks have been identified as a result of implementing this, Policy.

1.6 Equality Impact Assessment

An assessment has been undertaken, no adverse effects have been identified for staff, patients or the public as a result of implementing this Policy.

1.7 Maintenance

This Policy will be reviewed every 3 years or sooner if changes in legislation or guidance require. There must be a joint review between Information Governance and Information Security Leads. Responsibility lies with the Information Governance Steering Group for review and ratification of the policies.

1.8 Communication and Training

Approved Trust policies will be made available to staff via the Trusts Intranet page.

All staff must complete Information Governance Training on an annual basis via Trust Induction and/or Mandatory training days. Please see OP41 Induction and Mandatory Training Policy. Where necessary to support specific roles and responsibilities a training needs analysis shall be reviewed by the IGSG. OP41 will be implemented and communicated through the work of the IGSG. This Policy will be also implemented by the Information Governance Strategy which will set standards and a framework for monitoring.

The IG Training will be reviewed on an annual basis by the IG lead in line with any developments within the NHS England online training guidance and the DSP Toolkit. The IGSG is responsible for approving the IG training in line with NHS England guidelines. The training will include an assessment of compliance, of which there will be multiple assessments available for staff to complete. Training will also

be available via the Trust's my Academy for staff to complete the training online; the online assessment and training package must be updated on an annual basis.

1.9 Monitoring Process

Each individual sub policy will outline how its requirements and procedures will be monitored. At a high-level overall Information Governance compliance will be monitored as follows:

Criterion	Lead	Monitoring method	Frequency	Committee/ Group
Final DSP Toolkit position	Caldicott Guardian	QSOG Assurance Report/Chairman Summary	Annual	Quality committee
DSP Toolkit compliance	Requirement Leads	Online evidence submission	3 times annually	IGSG
DSP Toolkit Action plans	Objective Leads	Report	Monthly	IGAG
DSP Toolkit progress report	IG lead/DPO	Exception report	3 times annually	Quality committee
IG Incidents and breaches	IG Manager	Report	Bimonthly	IGSG
Independent review of DSP Toolkit self-assessment	Internal auditors	Report	Annual	Audit Committee

1.10 Auditing

Information Governance Spot-Check Audits will be completed across the Trust throughout the year, (see Attachment 9 for audit template). The outcome of the audits will be reviewed by the IGSG on a quarterly basis, any immediate issues where non-compliance will result in an incident must be raised with the department manager and the recommendations followed up by the IG Action Group.

1.11 References – links to other linked policies and procedures

Name of policy or procedure	Detail	Link
Data protection Procedure	Detail how the Trust meets its legal obligations and NHS requirements concerning the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).	Procedure 1
Data Protection Impact Assessment (DPIA) Procedure	Data Protection Impact Assessment (DPIA) to assess the implications of Privacy and Data Protection as a part of the design and implementation of any new system or process that involves the use of identifiable data. To enable an organisation to address the privacy concerns and risks, a DPIA must be conducted and documented to support the principle of accountability,	Procedure 2
IG / Data Security and Incident Procedure	This details how the trust meets its legal obligations and NHS requirements concerning General Data Protection Regulation (GDPR)and the Data Protection Act 2018. This procedure explains the incident process for reporting data security incidents and breaches.	**Procedure** 3
Information Asset Management and Procedure	Information Asset Management and Data flow	**Procedure 4**
National Data Opt Out Procedure	The national data opt-out allows a patient to choose whether or not they will allow their confidential patient information to be used for purposes beyond their individual care and treatment, for example, for research or planning purposes. This Policy allows service users, or the persons acting for them by proxy, control over setting or changing their own opt-out choice. They may change their mind at any time.	**Procedure 5**
Confidentiality code of conduct	Policy provides detail on: • Confidentiality compliance to law and guidance. • Expectations of staff for maintaining confidentiality • Maintaining confidentiality in practice	OP97 Confidentiality Code of Conduct for staff

	• Disclosing information to others for care and non-care purposes • Dealing with request for patient information form the media or police • Transferring/Sharing information safely by post, phone, fax, transport (safe havens) including flowcharts to use	
Information sharing policy and procedure	Policy provide detail on: • Circumstances where we must share information • How to reach a decision on sharing information • What to do for one off instances of sharing • Template agreements to use when sharing • Sharing and getting people's consent • Rules for sharing for care and non-care purposes	OP85 Information Sharing Policy
Freedom of information policy	The Freedom of Information Act 2000 (FOI) & Environmental Information Regulations 2004 (EIR) gives members of the public a general right to request access to all types of recorded information held by public authorities, promoting a culture of openness and accountability across the public sector.	OP90 Freedom of Information Policy
Corporate records Procedure	This procedure relates to all non-clinical operational records, also called corporate records, held in any format by the Trust. These are all administrative records such as personnel, estates, financial and accounting records, notes associated with complaints etc.	PR_02 Corporate Records Management Procedure
Health Records policy	Information contained within the health record is critical to the delivery of safe and appropriate health care. For the purposes of this policy the health record is the legal document relating to an individual's care and treatment, regardless of the format this is available in e.g. paper, electronic, clinical images etc. The purpose of this policy is to provide a structure to ensure adequate health records are maintained and that all aspects of an individual's health record, in any format or media type, from creation through to destruction, are controlled effectively to comply with legal and operational needs.	OP07 Health Records Policy
IT Cyber Security	The purpose of the IT security policy is to protect the security of the Trust's information	GOP06 IT Security Policy

group policy (GOP06)	assets and to ensure all staff are made aware of good practice surrounding the security of corporate and personal information.	
De-identification and Pseudonymisation policy	Provides guidance for all Trust personnel who use patient data as to how this will be used in a de-identified form for secondary (non-patient care related, defined below) use.	OP111 De-identification and Pseudonymisation Policy
Profiling, automated decision making and artificial intelligence policy	GDPR introduces provisions to ensure that profiling and automated individual decision making (whether or not this includes profiling) are not used in ways that have an unjustified impact on individuals' right	OP112 Profiling, Automated Decision Making and Artificial Intelligence Policy

1.12 Other Sources

NHS England – Information Governance and Data Protection Guidance - Practical IG guidance for NHS organisations, including access to records, lawful data sharing, transparency, and staff responsibilities. [england.nhs.uk]

Department of Health (2010) A question of balance: independent assurance of information Governance returns
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_121640

Code of Practice on Confidential Information (NHS England / NHS Digital, last updated May 2025)

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care

The Records Management Code of Practice for Health and Social Care (dec 2023)
https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

The Information Commissioners Office
https://ico.org.uk/

Data Security & Protection Toolkit
https://www.dsptoolkit.nhs.uk/

Reference Number and Policy name: OP13 Information Governance & Data Protection Policy	**Version:** **8.2** **August 2026**		**Status:** **Final**	**Author: Head of Data Security/ DPO** **Director Sponsor: Group Chief Medical Officer**
Version / Amendment History	Version	Date	Author	Reason
	V1.0	March 2008	Information Governance Manager	Policy creation
	V2.0	March 2010	Information Governance Assistant	Policy review due
	V2.1	June 2012	IG Manager	Policy review due
	V2.2	June 2012	IG Manager	Consultation with IGSG governance department
	V3	June 2012 Aug 2012	IG Manager	Trust wide consultation Policy committee Members
	V3.1	Oct 2014	IG Manager	Policy Review in line with DSP Toolkit v11 and review of GOP06. Update following comments from Compliance Manager
	V4.0	March 2017	IG Manager	Policy review due, and changes in legislation (GDPR) Amalgamation of all related IG Policies
	V 5.0	Feb 2019	IG manager/ DPO	Review policy
	V6.0	April 2019	IG manager/ DPO	Review policy
	V7.0	July 2020	IG manager/ DPO	Updated links to other policies and addition of appendix B /C

	V7.1	October 2023	IG manager / DPO	Extension
	V7.2	March 2025	IG manager / DPO	Extension
	V7.3	October 2025	IG manager / DPO	Extension
	V8.0	January 2026	IG manager / DPO	Review Policy
	V8.1	August 2026	IG manager / DPO	Updated Procedures 1 and 3
	V8.2	August 2026	IG manager / DP	Updated Procedures 1 and 3 and minor update to policy

Intended Recipients: All staff	
Consultation Group / Role Titles and Date: IGSG, IT, Policy Committee	
Name and date of Trust level committee where reviewed	Group Policy Meeting Membership – May 2026 Executive Sponsor Approval – July 2026 Chief Officer Sponsor approved minor updated – August 2026 – Version 8.2
Name and date of final approval committee	Group Policy Meeting Membership – May 2026 Executive Sponsor Approval – July 2026 Chief Officer Sponsor approved minor updated – August 2026 – Version 8.2
Date of Policy issue	August 2026
Review Date and Frequency (standard review frequency is 3 yearly unless otherwise indicated)	July 2029 – Every 3 years
Training and Dissemination: Policy will be made available to all staff on Trust intranet page, Information Governance Mandatory Training required annually.	

To be read in conjunction with: All list sub polices in appendices: Data protection Policy Confidentiality Code of Conduct for staff. Information Sharing Policy Freedom of Information Policy Non-Clinical Records Policy Heath Records Policy Breach Reporting Policy Pseudonymisation Policy	
Initial Equality Impact Assessment (all policies): **Completed Yes** **Full Equality Impact assessment (as required):** **Completed NA**	
Contact for Review	Head of Data Security & Protection
Implementation plan / arrangements (Name implementation lead)	Information Governance Manager
Monitoring arrangements and Committee	Information Governance Steering Group
Document summary / key issues covered: Changes to the law and ways in which staff process data in line with the New Data Protection Act 2018 and General Data Protection Regulation 2016. Provide staff with high level principles and links to sub polices which contains the details of the process staff are required to implement.	

Procedure 1 – Data Protection Procedure

2.1 Scope

This Data Protection Procedure describes how the Trust meets its statutory and NHS obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) and the

The Data Protection Act (DPA) 2018 is the core legal framework that protects personal data and individual rights in the UK. The Data Use and Access Act (DUAA) 2025 is a reform and enabling Act that amends and builds on the DPA 2018 and UK GDPR, focusing on how data can be used and shared safely, particularly to improve public services, innovation, and interoperability. They work together — the DUAA does not replace the DPA. For the purpose of this procedure, they will be referred to collectively as Data Protection Laws.

The Trust is a Data Controller and is therefore responsible for ensuring that all personal data is processed lawfully, fairly and transparently, and in accordance with the data protection principles set out in the UK GDPR. These principles govern how personal data is collected, used, stored, shared, and retained, and apply to all personal data processed by the Trust, regardless of format or medium.

This Procedure applies to all personal identifiable information across the Organisation, including but not limited to:

- Patient information
- Staff, the public and service user information
- Students, trainees, apprentices and volunteers' information

The Procedure covers all forms of information and information systems, including (but not limited to):

- Record systems purchased, developed, hosted or managed by or on behalf of the Trust
- Manual and paper-based records
- Computer and clinical systems
- Videos, audio recordings and other automated media
- Microfiche and film
- Paper and electronic records
- X-rays, scans and all other diagnostic and clinical images

By law, the Trust, its employees, contractors, and any third-party processors acting on its behalf must comply with the principles of data protection when processing personal data.

The Trust is required to:

- Maintain accurate and up-to-date records of all personal data processing activities

- Make such records available to the Information Commissioner's Office (ICO) on request
- Ensure appropriate technical and organisational measures are in place to protect personal data against unauthorised or unlawful processing, loss, damage or destruction

Data Protection Laws provide individuals ("data subjects") with specific rights in relation to their personal data. These rights include, but are not limited to:

- The right to be informed about how their data is used
- The right of access to personal data held about them
- The right to rectification of inaccurate or incomplete data
- The right to restrict or object to processing
- The right to erasure, where applicable
- The right not to be subject to decisions made solely by automated processing
- The right to prevent processing where it is likely to cause damage or distress and is not legally justified

The Trust is committed to ensuring that all personal data is processed in line with these rights and that robust governance, accountability and assurance arrangements are in place to demonstrate compliance.

All workforce members, including employees, contractors, agency staff, volunteers, and students, must only access, use, and disclose personal data where there is a legitimate work-related purpose and appropriate authorisation to do so. Accessing, viewing, querying, amending, sharing, disclosing, or otherwise using personal data without a lawful business need, or beyond the scope of an individual's role and responsibilities, constitutes inappropriate access and/or disclosure and is prohibited and can constitute as gross misconduct.

Inappropriate access or disclosure includes, but is not limited to:

- Accessing the records of patients, service users, colleagues, family members, friends, or any other individual without a legitimate business reason.
- Accessing one's own patient, employee, occupational health, HR, or other personal records through Trust systems outside approved access routes or self-service facilities.
- Accessing personal data out of curiosity or personal interest.
- Sharing personal data with individuals who do not have a legitimate need to know.

- Disclosing personal data verbally, electronically, or in writing without appropriate authorisation or a lawful basis.
- Sharing login credentials or using another individual's account to access information.
- Attempting to bypass security controls, access restrictions, or audit arrangements.

Staff wishing to access information relating to themselves must do so through the appropriate patient access, subject access request, HR, occupational health, or other approved processes.

Any suspected or actual inappropriate access to, or disclosure of, personal data must be reported immediately in accordance with the Trust's Data Security Incident Reporting Procedure 3.

All incidents will be investigated and may result in disciplinary action, referral to professional regulatory bodies, termination of contracts, and/or legal action where appropriate.

2.2 Accountabilities

All staff have a personal responsibility to comply with this Procedure and related Information Governance policies and procedures. Failure to do so may result in disciplinary action, up to and including dismissal, and may also lead to civil or criminal proceedings.

This Procedure applies to all staff, and external contractors who are employed to carry out work on behalf of The Trust, whether this is a temporary or time limited capacity. 3rd parties will be notified of their duties in the terms and conditions of their contract. Each individual is responsible for ensuring that they comply with relevant legislation and guidance for protecting the data they use.

2.3 Data Protection Principles

2.3.1 Lawful, Fair and Transparent
Individuals must understand what you will be doing with their data, it should be easy to find out and comply with the law. The Trust must proactively publicised this information at every opportunity.

2.3.2 Purpose Limitation
Data collected for a specific reason may only be used for that reason. If data is to be used for other reasons, it must be communicated clearly before using it to make it fair.

2.3.3 Data Minimisation
Always look to use the smallest quantities of personal data in order to complete a task. All data used should to be relevant to the processing purpose.

2.3.4 Accuracy
All data stored should be accurate and kept up to date. If inaccuracies are identified, reasonable steps to correct the data need to be made. This is a processed as a rectification request.

2.3.5 Storage Limitation
Information should not be kept longer than is necessary for the purposes for which the personal data is processed, whatever the format. Retention periods should be complied with at all times.

2.3.6 Integrity and Confidentiality
There must be appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction of data

2.3.7 Accountability
The Trust is lawfully obligated to show compliance with the above principles. Everyone processing data should document processing activities and be able to provide evidence of their activities upon request. This includes evidence such as privacy impact assessments on new projects, Information asset registers, data flow mapping and contracts with providers.

For more details on the application of the principles see Attachment 1

2.4 Legal basis for processing data

As a data controller the Trust must establish and publish the lawful basis that they are relying on for processing personal data and data that is special categories (sensitive data). Every service processing personal or special category data must ensure they document (in their asset register – see **section 2.8 below**) and communicate (via a fair processing notice – see section **2.6.1 Transparency**) which lawful basis they are relying to process data.

The GDPR sets out conditions for lawful processing of personal data (Article 6) and further conditions for processing special categories of personal data (Article 9) as listed below. If you are processing data relating to criminal convictions an Article 10 provision must also be satisfied.

Where there is a legal basis to process personal data for the provision of patient care or treatment, organisations should not rely on consent as the lawful basis for processing. Instead, it is essential to clearly identify the applicable legal basis in law and communicate this transparently to data subjects. Consent should only be used as the lawful basis for processing personal data where no other legal basis applies. This is because consent confers additional rights on data subjects, including the right to withdraw consent at any time, which may restrict or prevent further processing of the data and impact the organisation's ability to deliver services effectively.

For a breakdown of the legal bases relied on for processing see **Attachment 2** Legal bases table section for more detail.

2.5 Consent (Explicit consent)

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance reputation.

The GDPR definition of consent in Article 4(11) requires that:

This definition requires **all** of the following elements to be met:

Consent must be:

- **Freely given -** The individual must have genuine choice and control. Consent is not valid if there is imbalance of power, coercion, or detriment for refusing or withdrawing consent.
- **Specific -** Consent must be given for a clearly defined purpose (or set of purposes). Blanket or open-ended consent is not valid.
- **Informed -** The individual must be provided with clear information about:
    - Who is processing their data
    - What data will be processed

- For what purpose
- Their right to withdraw consent

- **Unambiguous -** Consent must be demonstrated through a **clear affirmative action**. Silence, inactivity, or pre-ticked boxes do not constitute consent.
- **Indicated by a statement or clear affirmative action -** Examples include signing a consent form, ticking an opt-in box, or clearly agreeing verbally where this is appropriately documented.

GDPR then, individual's consent must be sought. Consent should not be used if a valid lawful basis exists.

Whilst consent may not be relied on for processing, there is still a requirement to inform the individual about how their data is being used **(see section 2.6.1 transparency)**

2.5.1 Consent and the Common Law (Implied consent)

If consent is not required under GDPR because another lawful basis exists (see section 2.3), common law consent is still necessary to comply with the Common Law Duty of Confidence (confidentiality). For the purposes of common law, implied consent may be relied upon. This is consent which is not expressly granted by a person, but rather implicitly granted by a person's actions and the facts and circumstances of a particular situation – such as attending the emergency department or a GP.

Implied consent is not a satisfactory standard for data protection law, as explained in section (2.4) as it must be an explicit **clear affirmative action.**

2.5.2 Using consent and the interaction with other Rights

Where consent is used to allow the lawful processing under GDPR, the following controls and considerations **MUST** be put in place:

a. the requirement to facilitate withdrawal of consent – it must be as easy to withdraw as to give consent. This is known as **Opt Out.**

b. the requirement that the Trust must be able to demonstrate that consent has been obtained. Consider where consent is recorded and ensure consent is dated so it is understood when it was obtained.

c. the availability of the following rights (see rights in section 2.5):

   i. the right to erasure (where the subject withdraws consent and there is no overriding legitimate grounds to continue processing the data)

   ii. the right to data portability.

2.5.3 Expiry of consent

In general once an individual has given consent, that consent may remain valid for an indefinite duration, unless the individual subsequently withdraws that consent. For the purpose of this Procedure, the consent duration should be time limited to the specific 'piece of work' that is being proposed. It should be considered good practice to seek 'fresh' consent once the original piece of work is completed or there are significant changes in the circumstances of the individual or the work being undertaken.

2.5.4 Refusal and withdrawal of consent

If an individual makes a voluntary and informed decision to refuse consent for their personal information to be shared, this decision must be respected unless there are sound legal grounds for not doing so. A individual, having given their consent, is entitled at any time to subsequently withdraw that consent. Like refusals, their wishes must be respected unless there are sound legal grounds for not doing so. If an individual refuses or withdraws consent the consequences of doing so should be explained to them but care must be exercised not to place the person under any undue pressure.

Example consent forms can be found in - Attachment 3

2.6 Data Subject/ Individual Rights in relation to information

This Procedure sets out the high level principles in relation to Data Subject Rights, but must be read in conjunction with OP07 and HR polices, for how these rights apply to patient and staff records.

All rights that are listed below must be actioned within one month, unless stated otherwise. This can be extended by two months where the request for is deemed as complex. Complex request criteria will be defined in the above mentioned polices. A fee cannot be charged for processing of the request unless stated otherwise in this Procedure or supporting polices.

A request can be received both verbally and in writing so processes must be in place to ensure request can be logged and processed within the stipulated timeframes.

2.6.1 Transparency and the 'Right to be informed' – privacy notice

Individuals have the right to be informed about the collection and use of their personal data. The right to be told is also commonly referred to as a fair processing or privacy notice and is one of the most important rights. Regardless of what other rights apply to processing, the right to be told is fundamental to all rights being assessable by an individual. Done correctly the 'right to be told' about how information relating to the data subject is processed, should facilitate the use of data rather than hinder its use.

2.6.1.1 Privacy Notice Content

The following information must be communicated in the form of a privacy notice:

- The name and contact details of the Trust
- The name and contact details of our representative (if applicable)
- The contact details of our data protection officer
- The purposes of the processing
- The lawful basis for the processing
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to)
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable)

- The retention periods for the personal data
- The rights available to individuals in respect of the processing, **(see section 2.5).**
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

A template privacy notice can be found in toolbox – Attachment 4

2.6.1.2 When to communicate privacy notice information

This information must be provided to individuals at the time their personal data is collected. If personal data is obtained from other sources, such as another organisation, individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.

2.6.1.3 How to communicate privacy information

It is often most effective to provide privacy information to individuals using a combination of different techniques including layering website notices, dashboards, and just-in-time notices in the form of leaflets and posters.

- **A layered approach** – short notices containing key privacy information that have additional layers of more detailed information as per section 2.6.1.1 above.
- **Dashboards** – preference management tools that inform people how their data is used and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time individual pieces of information about people are collected. This is useful for research or project based data collection.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures

- **Literature** – Providing leaflets with privacy information supported by posters or targeted literature in patient/ staff areas.

2.6.2 Right of Access to Information

Individuals have the right to access their personal data and supplementary information such as audit data or Metadata (data about the data). The right of access allows individuals to be aware of and verify the lawfulness of the processing.

As a minimum a data subject can make a subject access request and is entitled to receive in full:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see section 2.5).

Information must be provided within one month of receipt free of charge. However, a 'reasonable fee' can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. For more details on how to make a request and when these conditions apply refer to the following

2.6.3 Right to Rectification

Individuals are entitled to have personal data rectified if it is 'factually' inaccurate or incomplete. Where the information in question has been disclosed to others, each recipient should be contacted to inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

2.6.4 Right to Erasure

The right to erasure is also known as the 'right to be forgotten' introduces a right for individuals to have personal data erased. A request for erasure can be made verbally or in writing, therefore processes should be put in place to ensure both types of request can be logged and monitored. The right to erasure is not an absolute right and should only apply in the following circumstances:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed;
- consent was the lawful basis for holding the data, and the individual withdraws their consent;
- legitimate interests was the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the data is processed for direct marketing purposes and the individual objects to that processing;
- the personal data has been processed unlawfully (ie in breach of the

lawfulness requirement of the 1st principle);

- comply with a legal obligation; or
- the personal data is being processed to offer information society services to a child.

2.6.5 Right to Restrict Processing

The right to restriction allows an individual to request the restriction or suppression of their personal data. This right is closely linked with the right to rectify and the right to object. The right to restrict the processing of their personal data is not an absolute right and should apply in the following circumstances:

- the individual contests the accuracy of their personal data and the accuracy is being verified by the trust;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- the personal data is no longer needed in line with retention but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under section and you are considering whether your legitimate grounds override those of the individual.
- When processing is restricted, the personal data can still be stored, but cannot be further used or processed.

Where an applicant has made a request to **rectify (2.6.3)** or **object (2.6.7)** to processing of their data, then the individual may have a right to restrict processing whilst these rights are being assessed, so they should be considered at the same time. As a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question

2.6.6 Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The process should allow for moving, copying or transfer of personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability is not an absolute right and only applies:

- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Therefore for care purposes, where data is processed under a statutory legal basis, the right to data portability would not apply. However where data is processed

under the performance of a contract, with the individuals consent or the processing involves automated means, this right should be facilitated.

2.6.7 Right to Object

The right to object to processing means that data should cease to be processed. This right should be considered in two parts:

2.5.7.1 Data protection / GDPR Objections

Individuals have the right to object to processing of there data where:

- Processing is based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); See section 2.3 for legal basis for processing).
- It is used for direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics (this does not include statutory reporting).

2.6.7.2 National opt out

NHS England developed a system to support the national data opt-out which provides patients more control over how identifiable health and care information is used. The system offers patients and the public the opportunity to make an informed choice about whether they wish their personally identifiable data to be used just for their individual care and treatment or also for research and planning purposes.

Patients and the public who decide they do not want their personally identifiable data used for planning and research purposes will be able to set their national data opt-out choice online.

Staff must be aware of where to sign post patients to, in relation to this type of opt-out which is additional to the right to object above. More guidance can be found in **Procedure 5- National data opt out**.

2.6.8 Rights relating to Automated Decision Making and Profiling

This is the process of making a decision solely by automated means without any human involvement, usually via a computer algorithm or formula. Profiling is automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.

Examples of this include:

- Risk stratification of patients based on frequency if attendance
- A recruitment aptitude test which uses pre-programmed algorithms and criteria.
- Use of AI

2.6.8.1 Article 22 gives individuals the right *not* to be subject to a decision that:

- is based solely on automated processing (no meaningful human involvement), and
- produes legal effects or similarly significant effects on them.

Automated decisions are only permitted if ONE of the following conditions applies:

- Necessary for a contract - The automated decision is necessary to enter into, or perform, a contract with the individual.

- Authorised by law - The decision is authorised by UK law, and that law includes appropriate safeguards for individuals' rights.

- Explicit consent - The individual has given explicit consent to the automated decision.

If any of the three conditions above are relied upon, Article 22(3) requires additional safeguards which include

- Meaningful Human intervention (Human in the loop such as a clinician checking the decision).
- Allow a data subject to express their point of view
- A mechanism for the data subject to contest the decision

If any of these techniques are used the following must be complied with:

- Send individuals a link the privacy statement data has been indirectly.
- Explain how people can access details of the information used to create their profile.
  - Tell individuals who provide their personal data how they can object to profiling, including profiling for marketing purposes.
  - Have additional checks in place for profiling/automated decision-making systems to protect any vulnerable groups (including children).
  - Only collect the minimum amount of data needed and have a clear retention policy for the profiles created.
  - Carry out a DPIA to consider and address the risks before starting any new automated decision-making or profiling.
  - Tell individuals about the profiling and automated decision- what information is used to create the profiles and where this information is from.

- Use anonymised data in profiling activities where possible.

2.7 ICO Data Protection Fee Notifications

Every organisation or sole trader who processes personal information is required to pay a data protection free to the Information commissioner's office ICO unless they are exempt. and ensuring the data protection fee is paid annually. The responsibility to register and be the liaison for the ICO will sit with the DPO.

2.8 Data Protection – Register of Processing activities ROPA (asset registers)

It is necessary that all data repositories pertaining to living people, held within the or on behalf of Trust, are identified, in order for the Trust to meets its obligations under Data Protection Laws.

Examples of data repositories include computer databases, manually held records, videotapes (typically used for clinical purposes) and CCTV tapes.

These will be identified though audits and development of information asset registers by anyone holding and processing data. All departments must engage when approached to complete a records audit/ asset register, the information provided will enable the Trust to:

- Observe fully the conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used, through validation and checking processes with patients. Please also see OP91 Data Quality Policy.

  Apply strict checks to determine the length of time information is held. See record management guidelines.
- Ensure that the rights of people about whom information is held can be fully exercised under the Act.
- Take appropriate technical and organisational security measures to safeguard personal information. GOP06 Information Security Policy
- Ensure that personal information is not transferred abroad without suitable safeguards.

For further guidance refer to **Procedure 4 - Information asset and data flow procedure.**

2.9 Data Protection Complaints Process

Under Article 164A DPA 2018 (inserted by DUAA), organisations must provide a complaints mechanism that addresses and complains made within the scope of relevant Data Protection Laws. The process should:

- Be easy to find, use, and access
- Can use existing complaints systems (no need for a standalone tool)
- Should be signposted in:
    - Privacy notices
    - DSAR responses
    - Websites
- Acknowledge the complaint within 30 calendar days of receipt
- Complaints should be Investigated without undue delay
- The complainant should be informed of progress
- There is no fixed statutory resolution deadline, but ICO guidance expects outcomes within 3 months, unless exceptional complexity applies. Seek advice from the DSP team in circumstances.
- Record keeping expectations – Complaints records should contain:
    - Date received
    - Date acknowledged
    - Issue raised
    - Actions taken
    - Outcome communicated

Procedure 2 – Data Protection Impact Assessment Procedure

1.0 Procedure Statement:

The Data Protection Impact Assessment procedure aims to detail how the Trust meets it obligations under Article 35 of GDPR mandates a statutory requirement to undertake a Data Protection Impact Assessment (DPIA) for the Trust to ensure privacy concerns and risks are appropriately recorded.

This procedure outlines how the trust identifies, assesses, and mitigates data protection risks in projects or activities involving the processing of personal data, in compliance with the UK GDPR and Data Protection Act 2018.

This DPIA Operating Procedure is applicable to any member of staff who are responsible for project managing a new “project” or “plan” to modify any existing system (information asset) or process. Any NEW projects and processes in the trust that involve processing of personal confidential data or the use of intrusive technologies that give rise to privacy issues and concerns. Such new projects and processes might include:

- Application/software
- Medical device
- The use of Artificial intelligence
- Study/research
- Data sharing initiatives

2.0 Accountabilities

2.1 Senior Information Risk Owner (SIRO) is the Trust’s Accountable Officer and has lead responsibility for the Trust’s information risks and provides a focus for the management of information risk at Board level. All high risk processing as identified through the DPIA process will be escalated to SIRO for decision.

2.2 Caldicott Guardian has responsibility for ensuring that information risks are assessed and mitigated to an acceptable level where it involves processing of patient data.

2.3 Data Protection Officer (DPO) assists in monitoring of internal compliance against GDPR including the application of Privacy by Design and any associated assessments. Also informs and advises on Data Protection obligations and provides advice regarding Data Protection. Will act as a contact point for data subjects and the supervisory authority (ICO). The DPO must be consulted as a matter of routine when a DPIA is carried out where it is considered high risk.

2.4 Information Asset Owners (IAO) who are responsible for ensuring that they services, systems and processes are assessed in line with this procedure and that

the services for this they are responsible are routinely carrying out DPIAs in a timely manner.

2.5 IG Steering Group has responsibility for decision making, providing guidance and recommendations to support on privacy and information security issues to wider Trust. Receive assurances from IGAG on the application of the DPIA review processes and any escalated risks.

2.6 Information Governance Action Group (IGAG) will monitor the DPIA log and any outstanding actions arising from the review of DPIAs from the DPIA reviewers' group. A DPIA risk report will be submitted quarterly. Any high risks and DPIA assessments of concern will be escalated to IGSG accordingly. This group will ensure continued improvement for the DSPT Toolkit and any other Information Governance Action Plans, which is fed back to the Information Governance Steering Group.

2.7 DPIA reviewers' group is a subgroup of the IGAG and will have delegated responsibility from IGSG to review submitted DPIAs and assign an assurance level based on the information submitted. All actions will be monitored and logged through to completion and any high risks and DPIA assessments of concern will be escalated to IGAG and IGSG accordingly.

3.0 Identify the Need for a Data Protection Impact Assessment (DPIA)

Staff must consider whether a DPIA is required whenever the trust plans to introduce, change or expand any systems, process, service or project that involves the use of personal data. A DPIA is mandatory under UK GDPR when processing is likely to result in high risk to individuals' rights and freedoms.

If staff are unsure if a DPIA is required, they must seek advice from the data protection and security team at the earliest stage, email rwh-tr.ig-enquiries@nhs.net for advice.

4.0 When Should You Start a DPIA?

A DPIA should begin prior to the processing or conducted as early as possible, in order that its findings and recommendations can be incorporated into the design of the processing operation. As the DPIA is updated throughout the lifecycle project, it will ensure that data protection and privacy are always considered and promote the creation of compliant solutions. The DPIA is an on-going process, especially where a processing operation is subject to change. Continual review should be expected and DPIA not considered one-time exercise

4.1 Who Should Carry Out a DPIA?

The Information Asset Owner is responsible for ensuring the DPIA is carried out by individuals with appropriate expertise and knowledge of the project" or "plan" to modify any existing system (information asset) or process within a particular service.

A DPIA should be carried out by the Trust where it involves data for which the Trust is a data controller. The Trust does not encourage third party suppliers or equivalent conducting DPIAs on behalf of the Trust as this may not consider the interests of the Trust and privacy risks and may not be adequately considered by a third party. This does not however exclude the involvement of a third party in terms of contributing to the assessment

Those conducting the assessment should also consult with other relevant individuals and stakeholders throughout the process, and where the processing is considered high risk, The DPO should be consulted as to whether the ICO should be notified of the assessment. For IT led projects, IT project team will be responsible for coordinating the DPIA and following up actions through to completion.

4.2 Core Elements of a DPIA

A DPIA must: describe the nature, scope, context and purposes of the processing, assess necessity, proportionality and compliance measures, identify and assess risks to individuals, and identify any additional measures to mitigate those risks. Below details the structure of how the assessment is carried out.

- Project Details (name, project lead, contact details etc.).
- Screening Questions.
- General Data Protection Principles (GDPR).
- Fair, Lawful and Transparent. • Processed for specific purpose(s) and not used for incompatible purposes (reasons for processing the information).
- Processing is adequate, relevant and necessary.
- Personal Information is not kept for longer than necessary (consider retention of information). • Personal Information is accurate, kept up to date and errors erased or rectified (consider provisions for deletions and rectifications).

- Appropriate measures to keep information secure.
- Information is processed in accordance with the wishes of the individual (individuals rights).
- Transfer of personal information outside the European Economic Area (EEA).
- Risk assessment following the above.
- Submit form for review – you must send email to IG Enquiries to advise your DPIA is ready for review.

4.3 Anonymised/Pseudonymised Data

Any systems/software which do not identify individuals in anyway do not require a DPIA to be completed. However, it is important to understand that what may appear to be anonymised data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that will not identity individuals.

4.4 DPIA Template

The DPIA assessment template is accessible via the following the link: Data Protection and Security which is within the pages from the intranet. Also see attachment 5 DPIA template.

Once a DPIA is completed, IG enquiries should be notified once the DPIA is ready for review. The DPIA will then be assigned to an IG officer for review and ensure all questions have been answered and that there is an enough information for the group to review. When you attend the DPIA review group you will present your DPIA to group and answers any relevant questions.

5.0 Information Assets and Data Flow Management

Information asset management is reviewed as part the DPIA review. All DPIA assessment that are completed must have a corresponding information asset mapped onto the Trust asset register.

6.0 Mitigating and Managing Risks

Any high risks within projects are monitored and reporting quarterly to IG Action group and any high risks DPIA assessments will be escalated to IGSG accordingly.

Procedure 3 – IG/ Data Security Incidents Procedure

1 Procedure Statement:

This IG/ Data Security Incidents Procedure sets out how the Trust meets its legal and regulatory obligations and NHS requirements in relation to the General Data Protection Regulation and the Data Protection Act 2018.

This procedure explains the incident reporting and management process to be followed by all staff, contractors, and third parties acting on behalf of the Trust for the reporting of:

- Data security/ Cyber incidents
- Personal data breaches
- Information governance incidents

The procedure ensures that incidents are identified, reported, assessed, managed, and escalated appropriately, in line with legal requirements, NHS guidance, and the Trust's Information Governance & Data Protection Policy.

2 Accountabilities

This Procedure applies to all staff, and external contractors who are employed to carry out work on behalf of The Trust, whether this is a temporary or time limited capacity. 3rd parties will be notified of their duties in the terms and conditions of their contract. Each individual is responsible for ensuring that they comply with relevant legislation and guidance for protecting the data they use.

2.1 Caldicott Guardian

The Caldicott guardian is a senior person responsible for protecting confidentiality of patients and service user's information. Caldicott guardian and SIRO will collectively advise and decide on the ICO reportable incidents.

2.2 Senior Information Risk Owner

The SIRO owns the Trusts' overall information risk policy and risk assessment process ensuring we have a robust incident reporting process for information risks. The SIRO reports to the Trust Board and provides advice on the content of the Trust's statement of Internal control in respect to information risk.

2.3 Data Protection Officer

The Data Protection Officer will reivew the incident and determine what the significant and likelihood of the data breach will be and whether this is reportable to the information commissioner's Office.

2.4 Data Security and Protection Team

The Data Protection and Security Team is responsible for ensuring all Data Security incidents are reported, reviewed, logged and investigated by the service as appropriate. Also making appropriate recommendations to managers of those services. Provide quarterly reports to the Information Governance Action group to report on any reoccurring themes and advise for processes to be put in place to minimise any recurring themes of the incidents.

2.5 Senior Managers

Senior Managers must ensure that employees within their area are aware of this process and do implement this process.

2.6 All staff

All staff are accountable for ensuring that they are fully aware of the actions to take in the event of a serious or reportable incident occurring, the criteria and timescale for reporting, investigation and management of such incidents and where to obtain assistance**.**

2.8 Information Governance Action Group

The IG action group has responsibility for monitoring and reviewing data security and protection incidents and related Trust policies and for overseeing the reporting process and confirming the grading assigned to incidents is accurate. They must also ensure that incidents are managed effectively and that appropriate steps are taken to minimise the risk of recurrence. This includes reviewing incident detail and trends using data and reports which are prepared each month by the IG Team for this purpose.

2.9 Information Governance Steering group

The IG Steering Group has responsibility for escalating data security and protection incidents. The reports from IG action Group will be tabled at IG Steering group and risks will be reported where required.

3 Data Security and Protection Incidents

3.1 What are the types of data breaches

Under the General Data Protection Regulation (GDPR), the European Data Protection Board (EDPB) categorises personal data breaches into three types:

- Confidentiality breaches – where personal data is disclosed or accessed without authorisation
- Integrity breaches – where personal data is altered or corrupted in an unauthorised manner
- Availability breaches – where personal data is lost, destroyed, or made unavailable in a timely manner

3.1.1 Confidentiality breach example

- Hacking or phishing attacks
- Sending personal data to the incorrect recipient
- Lost or stolen devices containing unencrypted personal data.
- Unauthorised access to data

3.1.2 Availability breach example

- Ransomware attack
- Server crash causing data loss
- Accidental deletion of files without back up.

3.1.3 Integrity breach example

- Incorrect record update- A doctor updates the incorrect record for a patient which could result in in appropriate treatment being prescribed.
- Software error- An electronic health record system experiences a bug that corrupts prescription records, altering dosages.

Further examples of Data Security and Protection incidents are provided in Appendix C of this document.

3.2 Incident Reporting

3.2.1 Reporting via the Trust Incident Reporting System

All staff must report information governance incidents via the incident reporting system (DATIX) and complete the required fields within DATIX. Under the Category, Information Governance, and select the appropriate subcategory from the list.

3.2.2 Reporting via the Data Security and Protection Team

The DSP Team will provide advice and guidance to staff who are unsure about reporting an incident or who has a concern about anything related to Data Protection and Security. The team can be contacted via email rwh-tr.ig-enquiries@nhs.net. If the DSP Team, consider the incident to be reportable the team will request the staff member to complete a root cause analysis report.

3.2.3 Reporting via the IT Help Desk Service

The incidents that involve the accessibility or availability of information held on the trusts IT system will be reported via the IT help desk. They may be contacted on extension 8888 or by logging IT issue: http://rwivantisd2a/HEAT. The DSP Team will only be notified of the incident if there is a risk to information security.

3.3 Incident Management Process

This procedure will the detail process for grading and investigating all IG/ Data Security incidents. The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has ***the potential to cause one or more*** of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

The DSP Team and the DPO will provide advice on what constitutes as ‘High Risk’.

3.3.1 Scoring Data Protection and Security Breaches

It is important to ensure data security and protection incidents are accurately recorded to ensure the right level of detail is captured. This requires timely and detailed information about the incident so an assessment can be made on severity, and advice can be provided accordingly.

All reported incidents must be initially scored by the handler/ manager assigned to the incident using the criteria set out in Appendix A. Incidents that score 2 or below will require a low-level investigation capturing causes and

learning within Datix. Incidents scoring 3 and above require full investigation using the RCA template in Attachment 6.

This will be reviewed by the DSP team to ensure scoring is accurate, and they reserve the right to change to reflect the severity.

Incidents scoring 3 and above will also be assessed against the ICO reporting criteria set out in Appendix B. This will be assessed and scored by the DSP team and a decision to report will be agreed by the Caldicott Guardian, SIRO and DPO. This must be done within 72 hours of being notified of the incident and having all the relevant information to report.

3.3.2 Recording and Classifying Data Security and Protection Incidents

All incidents will be classified under the relevant subcategory detailed in Appendix C.

3.3.3 Events having a Significant Impact on the Continuity of Essential Services (NIS Regulations)

The NIS Regulations define an incident as any event having an actual adverse effect on the security of network and information systems. Where there is an incident which involves a system or network which has a significant disruptive effect on health and care services, this may be reportable under these regulations via the Data Security and Protection Toolkit (DSPT). For example, an interruption to power supplies which affects medical equipment but does not affect health and care workers' access to data. What starts as a NIS incident may become a personal data breach, and some incidents may have the characteristics of both.

Any incident reportable under the NIS Regulations may also be reportable as a personal data breach under the GDPR reporting requirements set out in this guidance. Where this is the case the DSPT incident reporting tool will ensure that the incident is reported to both the ICO and the DHSC. When an incident is reported under both the NIS Regulations and GDPR the Department of Health and Social Care will work with the ICO to ensure appropriate consistency of approach and avoid unnecessary duplication. Criteria for assessing a NIS incident is set out in Appendix D. This relates to unexpected/additional fatalities caused by the impact of a network and information systems.

3.3.4 Incident Investigation

An incident must be investigated to determine the cause and harm that can or has resulted from the incident. The allocated incident hander will consider the below questions when investigating the incident. This is not an exhaustive list and there may be other questions

analysis report should be completed by the service the incident has occurred and whether this requires to be externally reported. The below outlines what should be considered when assessing the incidents:

- **Context -** Where and how the breach has occurred**.**
- **Scale -** How many individuals and records have been affected.
- **Sensitivity -** Type and risks level of the data involved**.**

- What has happened?
- How did you find out?
- When did you find out?
- Who was involved?
- Who is affected?
- When did the incident start?
- Is the incident still on going?
- How many citizens are affected?
- Have data subjects or users been informed?
- Is it likely that citizens outside England will be affected?
- Have you informed the Police?
- What other actions have been taken or are planned?
- What is the likelihood that people's rights have been affected?
- What is the severity of the adverse effect?
- Has there been any potential clinical harm as a result of the incident?
- Has the incident disrupted the delivery of healthcare services?
- Was the incident caused by a problem with a network or an information system?
- Which of these services are operated by your organisation?
- Have you notified any other (overseas) authorities about this incident?

3.3.5 Evidence collection and considerations during investigation.

The investigation will include collecting evidence relevant to the incident, recording the facts and follow up actions. Evidence may include audit trial, written statements from staff/ patients. When considering the evidence, you should:

- Identify and secure all relevant systems, records, and data sources at the earliest opportunity.
    - Prevent deletion, alteration, or overwriting of data by suspending automated deletion or retention jobs where appropriate
    - Restricting system changes that may impact the evidence
    - Consider suspending access to systems or data to ensure no further risk to the data or data subjects. Seek advice from DSP team on this.

- Preservation of Original Evidence - Original data must be preserved in its unaltered state. Original evidence should not be edited, annotated, or altered. Where copies are required:
    - Create read-only or forensic copies wherever possible
    - Clearly label copies as “working copies”
- Limit access to investigation materials to authorised individuals only
- Apply the principle of least privilege, granting access solely on a need-to-know basis. Record:
    - Who has accessed the data
    - When access occurred
    - The purpose of access
- Maintain a clear chain of custody for all evidence, documenting:
    - What data was collected
    - When and from where it was collected
    - Who handled it
    - Where and how it was stored
- Any transfer of evidence must be authorised, documented, and traceable
- Apply version control to investigation documentation to avoid confusion or inconsistency
- Ensure documentation is dated, attributed, and stored securely

3.3.6 Follow up actions

Following the incident investigation, the follow up actions may include:

- Referral to Patient Liaison Service where this concerns a Data subjects care.
- Referral to Human Resources Department where it concerns the conduct of a member of staff.
- Trust wide learning to be circulated amongst staff whether this is an individual department or the trust.
- Ensuring actions are audited to ensure they are working.

3.6 Reporting and Notification of Incidents

3.6.1 Internal Reporting

Incidents must be reported via the Trust Incident reporting system as soon as they become known so that investigation and containment can start. See section 3.2 above for detail on how to report.

The Caldicott Guardian, SIRO and DPO will be notified of all serious incidents for consideration of escalation to the ICO.

The IG Steering group will receive regular assurances on incident reporting and mitigations and actions.

3.6.2 External Reporting

Where an incident is deemed serious, it will be reported to the ICO and relevant bodies via the DPO on the Data Security and Protection Incident Reporting Too, which is an online system imbedded within the Data Security and Protection Toolkit (DSPT). This tool has been agreed by NHS England and the ICO for reporting personal data security breaches.

Dependant on the responses to the questions contained in the reporting tool, the information provided will be sent to the ICO, the DHSC and the National Cyber Security Centre.

3.6.3 Notification to the Data Subject

Article 34 of GDPR requires any personal data breach, that is likely to result in a high risk to the rights and freedoms of individuals, to be communicated with those affected. Any communication must contain the following four elements:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other
- contact point from whom more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken or proposed to be taken by the
- controller to address the personal data breach, including, where
- appropriate, measures to mitigate its possible adverse effects

A communication is not necessary in the following three circumstances:

- the controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach for example the data were encrypted.

- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.

- it would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website

4.0 Further guidance and appendices

The below is a list of other policies, procedures documents or guidance documents (internal or external) which employees should refer to for further details:

Name of document	location
General Data Protection Regulation 2016	**https://gdpr-info.eu**
Data Protection Act 2018	**http://www.legislation.gov.uk/**
Guide to the Notification of Data Security and Protection Incidents' provided by NHS Digital	**Data Security and Protection Toolkit**
The Security of Network & Information Systems Regulations (NIS Regulations) 2018	The NIS Regulations 2018 - GOV.UK
ICO - Personal data breaches: a guide	https://ico.org.uk/for-organisations/the-guide-to-nis/incident-reporting/ Personal data breaches: a guide | ICO

Appendix A- Criteria to assess a Data Security Incident

When assessing a Data Security Incident, the following factors should be considered to determine the severity and level of investigation that is required. All incidents need to be investigated, and learning documented regardless of the scoring.

The handler/ manager who is assigned the incident is responsible for initially scoring the incident using the below.

This will be reviewed by the DSP team to ensure scoring is accurate, and they reserve the right to change to reflect the severity.

Select one from each question

1 - How many data subjects could be affected:

Score	Number of data subjects affected
1	1-5
2	6-20
3	21-100
4	100+

2 - Sensitivity of data involved (See IG and DP policy for definitions of the below):

Score	Data description
0	Low risk (non-sensitive)
1	Personally identifiable data
2	Personally Identifiable **Special category** data (e.g. health, ethnicity, religion)
3	Highly sensitive (Childrens, safeguarding, sexual health)

3 – Additional factors to consider

Score	Additional factors + or – a factor to the score
-1	Sent to/ diverted by a trusted source • sent to another NHS body that is bound by NHS rules • information found/ obtained by staff and was contained
-1	Information was encrypted and password protected, reducing the risk of unauthorised access.

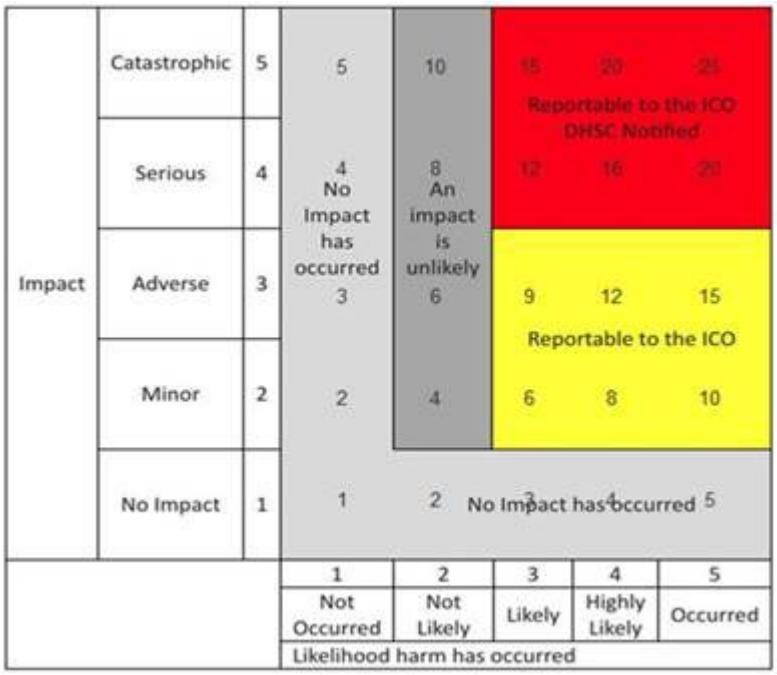
-1	Information was recovered, deleted, or recalled before being accessed by an unauthorised individual.
-1	The data is old, out of date or no longer relevant
-1	The data was recovered quickly and completely.
-1	The unintended recipient confirmed deletion and non-use of the information.
+1	Disclosed into the public domain
+1	Disclosed/ accessible to multiple sources/recipients
+ 1	Individuals affected are likely to experience substantial harm or distress, including significant embarrassment, detriment, or other serious impact, and may also have been placed at risk of, or actually incurred, physical harm or a clinical untoward incident.
+1	Failure to adequately implement, enforce, or comply with appropriate organisational and technical measures to protect information. In line with trust policies.

Scoring outcome

Incidents that score 2 or below will require a low-level investigation capturing causes and learning. Incidents scoring 3 and above require full investigation using the RCA template in Attachment 6.

Appendix B - When is an incident reportable to the Regulator under GDPR

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. Anything within the yellow box or red box will be reportable to the regulator ICO



Likelihood adverse effect occurred

Likelihood adverse effect occurred		
No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.

4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Severity of adverse effect on individuals

Severity of adverse effect on individuals		
No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Appendix C- Datix categorises

Categories when reporting a Data Security and protection incident. When choosing a category, you may find that several of the below categories apply. When considering the type of incident, you should select the category which is the main root cause of the incident occurring.

Disclosed in error – Post
This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This would include situations where the information **itself hasn't actually been accessed**. Examples include: Examples include: • Letters / correspondence / files sent to the incorrect individual • Patient information being sent to wrong person via post e.g. appointment letter • Patient files being sent to wrong destination
Disclosed in error - Fax
This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This would include situations where the information **itself hasn't actually been accessed**. Examples include: Examples include: • Info being sent to wrong department internally/ or external body • Info faxed to a member of the public in error • To the wrong recipient
Disclosed in error - Email
This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This would include situations where the information **itself hasn't actually been accessed**. Examples include: Examples include: • Email sent to wrong recipient internally • Info being emailed external to wrong recipient • Email in error to a member of the public
Disclosed in error – Other
Examples include: • Verbal disclosure to the wrong patient over the phone • Too much information/ detail disclosed (recipient may be correct) • Failure to redact personal data from documentation supplied to third parties; • Verbal disclosures made in error (however wilful inappropriate disclosures / disclosures made for personal or financial gain will fall within the s55 aspect of reporting); • Inclusion of information relating to other data subjects in error;

Lost in transit

The loss of data (usually in paper format, but may also include CD's, tapes, DVD's or portable media) whilst in transit from one business area to another location. May include data that is;

- Lost by a courier;
- Lost in the 'general' post (i.e. does not arrive at its intended destination);
- Lost whilst on site but in situ between two separate premises / buildings or departments;
- Lost whilst being hand delivered, whether that be by a member of the data controller's staff or a third party acting on their behalf

Generally speaking, 'lost in transit' would not include data taken home by a member of staff for the purpose of home working or similar (please see 'lost or stolen hardware' and 'lost or stolen paperwork' for more information).

Examples include:

- Files lost on way to ward/ health records
- Fax was not received
- Information sent by post but never received

Lost or stolen hardware

The loss of data contained on fixed or portable hardware. Examples may include;

- Lost or stolen laptops;
- Hard-drives;
- Pen-drives;
- Servers;
- Cameras;
- Mobile phones containing personal data;
- Desk-tops / other fixed electronic equipment;
- Imaging equipment containing personal data;
- Tablets;
- Any other portable or fixed devices containing personal data;

The loss or theft could take place on or off a data controller's premises. For example the theft of a laptop from an employee's home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk.

Lost or stolen paperwork

The loss of data held in paper format. Would include any paper work lost or stolen which could be classified as personal data (i.e. is part of a relevant filing system/accessible record). Examples would include;

- medical files;
- letters;
- rotas;
- ward handover sheets;
- employee records

The loss or theft could take place on or off a data controller's premises, so for example the theft of paperwork from an employee's home or car or a loss whilst they were travelling on public transport would be included in this category.
Work diaries may also be included (where the information is arranged in such a way that it could be considered to be an accessible record / relevant filing system).

Examples include:

- Patient files/ information cannot be found
- Patient files/ information stolen
- Parts of a paper record are missing

Non secure disposal hardware

The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include;

- Failure to meet the contracting requirements of principle seven when employing a third party processor to carry out the removal / destruction of data;
- Failure to securely wipe data ahead of destruction;
- Failure to securely destroy hardware to appropriate industry standards;
- Re-sale of equipment with personal data still intact / retrievable;
- The provision of hardware for recycling with the data still intact

Non secure disposal paperwork

The failure to dispose of paperwork containing personal data to an appropriate technical and organisational standard. It may include;

- Failure to meet the contracting requirements of principle seven when employing a third party processor to remove / destroy / recycle paper;
- Failure to use confidential waste destruction facilities (including on site shredding);
- Data sent to landfill / recycling intact – (this would include refuse mix up's in which personal data is placed in the general waste);

Uploaded to website in error

This category is distinct from 'disclosure in error' as it relates to information added to a website containing personal data which is not suitable for disclosure. It may examples such as;

- Failures to carry out appropriate redactions;
- Uploading the incorrect documentation;
- The failure to remove hidden cells or pivot tables when uploading a spread-sheet;
- Failure to consider / apply FOIA exemptions to personal data
- Data published on a website in error
- Social Media Disclosures

Security failing - Technical (consider if also NIS reportable)

This category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include but are not limited to:

- Failure to appropriately secure systems from inappropriate / malicious access;
- Failure to build website / access portals to appropriate technical standards;
- The storage of data alongside other personal identifiers in defiance of industry best practice;
- Failure to protect internal file sources from accidental / unwarranted access (for example failure to secure shared file spaces);
- Failure to implement appropriate controls for remote system access for employees (for example when working from home)
- Hacking
- Weak password administration

- System outage causing data loss/ corruption/ unavailability
- Virus causing data loss/ corruption
- DoS Denial of Service attacks

Security failing - Organisational or Procedural

Examples include but are not limited to:

- Failure to anonymise information where appropriate
- Failure to regularly review user access permissions
- Excessive access granted beyond job role requirements
- Delayed removal of access for staff who leave, change roles, or are suspended
- Poor procedures for sharing information internally or with third parties
- Lack of documented approval or authorisation processes

Unauthorised Access

Under section 170 of the Data Protection Act 2018, it is an offence for a person to knowingly or recklessly obtain, disclose, or retain personal data without the consent of the Data Controller, or to procure the disclosure of personal data to another person without lawful authority. This includes accessing personal data without a legitimate business need, even where the individual has technical access to the system.

Example
An employee with administrative access to a centralised system containing patient records accesses the record of a family member's associate out of personal curiosity. The employee has no legitimate work-related purpose for accessing the records and is not authorised to do so under Trust policies. The employee subsequently uses information obtained from the record for personal purposes. This constitutes unauthorised access and unlawful use of personal data and may represent a criminal offence under the Data Protection Act 2018, as well as a serious disciplinary matter.

Further Examples of Section 170 Offences

Examples of behaviour that may constitute unlawful access or disclosure include:

- Accessing patient, staff, or service user records without a legitimate business purpose
- Viewing records of family members, friends, colleagues, or acquaintances without authorisation
- Accessing systems or datasets beyond the permissions required for one's role
- Entering secured areas where confidential records are stored without authorisation
- Using valid login credentials to browse or search records out of curiosity
- Allowing others to access systems using your login details
- Collecting or sharing personal data outside approved processes or systems

Unauthorised Disclosure

Under section 170 of the Data Protection Act 2018, it is an offence for a person to knowingly or recklessly obtain, disclose, or retain personal data without the consent of the Data Controller, or to procure the disclosure of personal data to another person without lawful authority. This includes accessing personal data without a legitimate business need, even where the individual has technical access to the system.

Example

An employee with access to details of patients who have sought treatment following an accident, sells the details to a claims company who then use this information to facilitate lead generation within the personal injury claims market. The employee has no legitimate business need to view the documentation and has committed an offence in both accessing the information and in selling it on.

Unauthorised is the key part here. Examples include:

- Verbal or written disclosures that the **recipient** is not entitled to receive
- Phishing emails – disclosing information in response
- Social Media Disclosures
- Spoof website

Corruption or inability to recover electronic data

Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption of care / adverse clinical outcomes.
For example;

- The corruption of a file which renders the data inaccessible;
- The inability to recover a file as its method / format of storage is obsolete;
- The loss of a password, encryption key or the poor management of access controls leading to the data becoming inaccessible

Misfiling

Examples include:

- Documentation that appears in another patients record
- Documents indexed against another patient

DQ

Data quality incident include but are not limited to:

- Error in recording
- Illegible or incomplete
- Transpiration error
- Duplication of information/ records
- Merged in error
- Error In patient identification

Data subject rights

Data subject rights incidents could include but are not limited to the following:

1. Failure to Facilitate Data Subject Rights
Where the Trust does not appropriately enable individuals to exercise their rights, including:

- Failing to provide clear information on how to exercise rights
- Obstructing, discouraging, or placing unreasonable barriers on requests
- Requiring unnecessary verification or information

2. Failure to Respond Within Statutory Timescales
Where the Trust does not respond to a valid data subject request/ rectification of complaints under data protection within the required timeframe:

- **One calendar month**, unless a lawful extension applies
- Failure to notify the individual of an extension and reason

3. Failure to Provide Complete or Accurate Information
Where the response to a data subject request is:

- Incomplete
- Inaccurate
- Misleading
- Not provided in a clear, accessible, or intelligible format

This includes failure to supply all personal data within scope.

4. Unlawful Restriction or Denial of Rights
Where the Trust incorrectly refuses or limits a data subject's rights without a valid legal basis, including:

- Access
- Rectification
- Erasure
- Restriction of processing
- Objection

or fails to properly explain the lawful exemption relied upon.

5. Inaccurate or Unjustified Reliance on Exemptions
Where exemptions (e.g. health, safeguarding, management forecasts) are applied:

- Incorrectly
- Without documented justification
- Without appropriate proportionality consideration
- Without senior or DPO oversight

6. Failure to Rectify or Update Personal Data
Where inaccurate or incomplete personal data is not corrected:

- After a valid rectification request
- Within an appropriate timeframe
- Or where the individual is not informed of the outcome

7. Failure to Restrict Processing When Required
Where processing continues despite a valid request for restriction, for example:

- While accuracy is contested
- During consideration of an objection
- When required by law or regulatory guidance

8. Failure to Respect the Right to Erasure (Where Applicable)
Where personal data is not erased:

- Without a lawful reason to retain it
- After consent has been withdrawn (where applicable)
- Following the cessation of the lawful basis

9. Failure to Respect the Right to Object
Where the Trust continues processing personal data despite a valid objection and absence of overriding legitimate grounds, particularly in cases of:

- Non-direct care processing
- Secondary use of data
- Communications or profiling

10. Failure to Inform Individuals of Their Rights
Where individuals are not adequately informed about:

- Their rights
- How their data is used
- How to complain to the ICO

This includes inadequate or outdated privacy notices.

11. Failure to comply with Consent

A breach of consent occurs where personal data is processed in a way that does not comply with the requirements or conditions of valid consent under the UK General Data Protection Regulation (UK GDPR).
This applies only where consent is being relied upon as the lawful basis for processing (not where another lawful basis applies, such as public task or legal obligation).

1. Processing Without Valid Consent
2. Consent Not Freely Given
3. Consent Not Specific or Informed
4. Processing Beyond the Scope of Consent
5. Failure to Respect Withdrawal of Consent
6. Failure to Refresh or Review Consent
7. Inadequate Record-Keeping of Consent

Appendix D -Significant Impact Thresholds - Events having a Significant Impact on the Continuity of Essential Services (NIS Regulations)

Category	Criteria	Applies to	Rationale
Excess fatalities1	>0	All	Public safety
Excess casualties2	>0	All	Public safety
Potential clinical harm3	>50	All	Public safety
Closure or diversion of emergency departments – major trauma centre	>3hrs	Trust – major trauma centre	10% of population, 3 hours
Closure or diversion of emergency departments – all other orgs	>24hrs	Trust/independent provider – non major trauma centre	City, 1% of population, 24hrs
Outpatient appointments cancelled	1,500	Trust/independent provider	City, 1% of population, 12hrs
Inpatient episodes cancelled	250	Trust/independent provider	City, 1% of population, 12hrs
Lack of availability of NHS111 services4	>3hrs	NHS111 services	Region, 4% of population, 3hrs
Disruption to NHS emergency ambulance services	(a) ≥85% service degradation for ≥15 minutes	Ambulance	Ambulance Quality Indicators
	(b) ≥30% degradation for ≥35 minutes		
	(c) ≥5% for ≥4 hours		
Non-availability of drugs and/or medical devices	>24hrs	Trust/independent provider	City, 1% of population, 24hrs
Community care appointments cancelled	1,500	Trust/independent provider	City, 1% of population,

Procedure 4 – Information Asset Management and Data Flow Procedure

1.0 Procedure statement:

The Information asset management procedure aims to detail how the trust manages its information assets and data flows to ensure data is secure, accurate and used in compliance with legal and regulatory requirements. Documenting Information Assets or having a Record of Processing Activities (ROPA) is a legal requirement under the General Data Protection Regulations (GDPR) 2016 Article 30 – as well as supporting compliance with the Data Security and Protection Toolkit. It is important the Trust is aware of the information its holds, to ensure it is adequately protected and any risks are managed.

2.0 Accountabilities

2.1 Caldicott Guardian who has responsibility for ensuring that information risks are assessed and mitigated to an acceptable level where it involves processing of patient data.

2.2 Senior Information Risk Owner (SIRO) is the Trust's Accountable Officer and has lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level. All high risk processing as identified through the DPIA process will be escalated to SIRO for decision.

2.3 Data Protection Officer (DPO) to inform and advise the Trust on its obligations under GDPR, monitor regulation compliance. Any information asset data breaches need to be reported to the DPO by the Information Asset Owner as soon as they become aware to ensure investigations have implemented and the Information Commissioners officer have been notified within 72 hours of the breach.

2.4 All staff follow the appropriate data handling procedures and report any changes or incidents.

2.5 Information Asset Owners (IAO) who are responsible for ensuring that they services, systems and processes are assessed in line with this procedure and that the services for this they are responsible are documenting Information Assets in a timely manner.

2.6 Information Asset Administrators (IAA) provide the support to the IAO in ensuring the assets are mapped and managed. This will include managing access and permissions to information assets, reviewing their controls and documenting this in the Information asset register. (IAR).

2.5 Information Asset Management group will monitor the information assets within the Trust that are held on each of services Information asset register and highlight the risks that are identified within.

2.6 What is an Information Asset?

An information asset is a body of information that is defined and managed as a single unit so that it can be understood, shared, protected, and used effectively.

Information assets include any collection of data required to support the organisation's business, clinical, or administrative functions used to create, store, process, or manage that information. An information asset may comprise one or more of the following:

- Electronic data held within information systems or databases
- Paper records or files
- Spreadsheets, reports, or datasets
- Emails or correspondence
- Images, audio, or video recordings

Information assets may exist in multiple formats and be created, stored, or processed through a wide range of mechanisms.

2.7 What is a Data Flow?

A data flow demonstrates all internal and external transfers of personal and sensitive information, it will record the source, method of transfer, frequency and purpose of processing.

2.8 What is required to be recorded

The Trust's ROPA will include, as a minimum:

- The name and contact details of the Trust (Data Controller), and where applicable:
- Joint Controllers
- Data Protection Officer (DPO)
- The purposes of the processing
- A description of the categories of data subjects (e.g. patients, staff)
- A description of the categories of personal data, including special category and criminal offence data where applicable
- The lawful basis for processing, and conditions for special category or criminal offence data
- The categories of recipients with whom personal data is shared (including external processors)
- Details of international transfers, where applicable, including safeguards used
- Retention periods or criteria used to determine how long data is kept

- A general description of technical and organisational security measures in place

2.9 DSPT Compliance

To meet DSPT evidence requirements, the Trust will:

2.9.1 Identify and document all information assets within scope of its processing activities

2.9.2 Maintain an Information Asset Register (IAR) that:

- Clearly describes the asset and its purpose
- Identifies whether personal or special category data is processed
- Records system ownership and data flows where applicable

2.9.3 Assign a named Information Asset Owner (IAO) for each asset, accountable for:

- Security and access controls
- Risk identification and mitigation
- Data quality and appropriate use

2.9.4 Ensure information assets are:

- Protected by proportionate technical and organisational controls
- Subject to regular review and risk assessment
- Managed in line with approved retention and disposal schedules

These arrangements support compliance with UK GDPR accountability, DSPT outcomes, and records management obligations.

3.0 Training

All staff that are identified as Information Asset Owner or Information Asset Administrator will be required to undertake the information asset management training. Details of this can be found on the Trust Intranet or from the DSP Team.

Procedure 5 – National Data Opt Out

5.0 What is the National Data Opt Out?

The national data opt-out allows a patient to choose whether or not they will allow their confidential patient information to be used for purposes beyond their individual care and treatment, for example, for research or planning purposes.

This Policy allows service users, or the persons acting for them by proxy, control over setting or changing their own opt-out choice. They may change their mind at any time.

5.1 When does the Opt Out apply?

This Policy sets out the approach that The Royal Wolverhampton NHS Trust (RWT) as a health care organisations when assessing whether the national data opt out applies.

Opt out applies where patient information is used for purposes **beyond** individual care also referred to as “direct care”.

Data sharing for individual direct care and treatment includes:

- Passing information from one care setting to another - for example when a GP refers a patient to a hospital for tests.
- local shared care records - put in place to help local health and care organisations share data with each other, for example to provide out of hours services or to improve patient safety when the patient is seen in different settings.
- Hospital Records - important patient information.

There are other elements of patient care which rely on the wider processing of data, but that should also be treated as individual care, and so not within scope of national data opt-out policy. These include:

- Population screening programmes - for conditions such as cervical and bowel cancer, which the UK National Screening Committee (UK NSC) has advised that the NHS should offer.
- Risk stratification used for case-finding - when carried out by a provider involved in an individual's care.
- Local audit of the safety and quality of care - when carried out by the professionals and team responsible for the care of the patient.

5.1.1. Opt out application

The national data opt-out applies to the disclosure of confidential patient information for purposes beyond individual care across the health and adult social care system in England. Such purposes include, but are not limited to:

- Where processing relies on Section 251 application. Section 251 of the National Health Service Act 2006 allows the Secretary of State for Health and Social Care to make regulations to authorise or require the processing of confidential patient information (CPI) for prescribed medical purposes and, in so doing, to set aside the common law duty of confidentiality. The only regulations made under this provision are the Health Service (Control of Patient Information) Regulations 2002, also known as section 251. Applications for section 251 can be found on the national register here https://www.hra.nhs.uk/planning-and-improving-research/application-summaries/confidentiality-advisory-group-registers/

- Planning such as predicting what services will be needed in the future, so funding and resources can be put into place or reviewing patient records to understand outcomes of patient care.

- Research such as reviewing multiple service user records or data sets to research diseases and illnesses and their treatments to see whether there are side effects or risk factors associated with certain medications, identifying risk factors for disease and its severity, or monitoring the effects of a new drug or type of treatment.

- The opt-out applies regardless of the format of the data and this includes structured and unstructured electronic data and paper records.

5.1.2. Opt Out exemptions

- The National Data opt out does not apply to aggregate data and patient health data for a local audit purposes.

- The Policy does not apply where consent has been gained for the activity.

- It does not apply to children's social care services or services outside of England.

- Consent - The national data opt-out does not apply where explicit consent has been obtained from the patient for the specific purpose.

- Communicable diseases and risks to public health - The national data opt-out does not apply to the disclosure of confidential patient information required for the monitoring and control of communicable disease and other risks to public health. Regulation 3 allows confidential patient information to be lawfully processed with a view to:

  - Diagnosing communicable diseases and other risks to public health
  - Recognising trends in such diseases and risks
  - Controlling and preventing the spread of such diseases and risks.
  - Monitoring and managing:
  - Outbreaks of communicable disease incidents of exposure to communicable

- Delivery, efficacy and safety of immunisation programmes
- Adverse reactions to vaccines and medicines
- Risks of infection acquired from food or the environment (including water supplies)
- The giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.

- Payments and invoice validation - National data opt-out does not apply to data used for payment and invoice validation purposes, invoice validation for non-contracted activities and for contracted activity anonymised data should be used.

- Risk stratification - The national data opt-out does not apply to data disclosures for risk stratification for case finding but does apply where support under S.251 and not where the data for risk stratification is anonymised in line with the ICO Code of Practice on Anonymisation.

- Overriding public interest - the national data opt-out does not apply to the disclosure of confidential patient information where there is an overriding public interest in the disclosure, i.e. the public interest in disclosing the data overrides the public interest in maintaining confidentiality.

- See national compendium for specific processing that may also be exempted where and assessment has been made on common uses where to show whether opt-outs need to be applied.

5.2 Interaction with other Opt-Outs

Prior to the launch of the national data opt-out individuals could set two types of general opt-outs, via their GP practice?

Type 1 opt-out prevents information that identifies individuals being shared outside of their GP practice, for secondary uses and continues to be honoured until 2020 when the Department of Health and Social Care (DHSC) will consult with the NDG before confirming their removal.

Type 2 opt-out prevented confidential patient information from being shared outside of NHS Digital for purposes beyond individual care which have been replaced by the national data opt-out and are no longer valid. All type 2 opt-outs recorded in GP practices up to and including 11 October 2018 have been migrated to become national data opt-outs.

GDPR opt out is separate this this ad is covered in the policy above.

5.3 How do patients register their Opt Out?

Where a patient has expressed a desire to opt out, they should be directed to the following location: nhs.uk/your-nhs-data-matters. This is managed by NHS digital.

5.4 What to do if opt out applies to your processing?

When the opt-out is applied, the entire record (or records) associated with that individual must be fully removed from the data being disclosed. The NHS number is used as the identifier for the removal of the records.

Where data flows or disclosures should have national data opt-outs applied, you need to:

- Check lists of NHS numbers against those with national data opt-outs registered – this is done via the technical solution detailed below.

- Have a process in place, when you get the results back, to ensure that you only use or disclose information for the returned list of NHS numbers, as any with national data opt-outs registered will have been removed.

5.4.1 Messaging exchange for social care and health (MESH)

National data opt-outs are held on the NHS Spine against an individual's NHS number. If your use or disclosure of data needs to have national data opt-outs applied, you must remove records for patients with an opt-out registered from the data being used.

The Trust has established a system to send files to the MESH via the information team so any data that is subject to this check should be sent to rwh-tr.infodep@nhs.net. You are required to submit lists of NHS numbers only and receive lists back with the NHS numbers removed for those patients that have opted out.

To help GP practices to become compliant with the national data opt-out, the four principal GP system suppliers have been commissioned to develop and embed the service into their clinical systems. Further information will be made available as the GP system suppliers confirm their delivery plans. See further information for GP practices.

Attachment 1

The seven Data Protection Principles are that:	What this means in practice
1) The processing of personal data must be lawful, fair and transparent	**Be open, honest and clear.** There should be no surprises, so inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with... • E.g. when formulating a research project remember to be open and transparent about what you will be doing with the information. • E.g. when working in a team, ensure that the patient/staff is aware of who the members of the team are, and that all those involved with their care may need to see their notes. In order to comply with this principle, fair processing notices/ privacy notices are required to be made available to staff and patients to advise them how their data is being processed and what rights they have relating to that processing. For more information see **heath records policy/ HR policy**
2) The purposes of processing be specified, explicit and legitimate	**Only use personal information for the purpose(s) for which it was obtained.** Only share information outside your practice, team, home, ward, department or service if you are certain it is appropriate and necessary to do so. If in doubt, check first! • E.g. personal information on a Patient Administration System must only be used for healthcare purposes - not for looking up friends' addresses or birthdays or your own information.
3) Personal data be adequate, relevant and not excessive	**Only collect and keep the information you require.** It is not acceptable to hold information unless you have a view as to how it will be used. Do not collect information "just in case it might be useful one day!" • E.g. taking both daytime and evening telephone numbers if you know you will only call in the day. • Explain all abbreviations • Use clear legible writing • Stick to the facts - avoid personal opinions and comments
4) Personal data be accurate and kept up to date	**What mechanisms do you have for checking the information is accurate and up-to-date?** Take care inputting information to ensure accuracy How do you know the information is up-to-date?

	• E.g. each time a patient attends a clinic, they should be asked to confirm that their details are correct - address, telephone number etc. • Check existing records thoroughly before creating new records • Avoid creating duplicate records
5) Personal data be kept for no longer than is necessary	**Follow retention guidelines** • Check your organisation's retention policy • Ensure regular housekeeping/spring cleaning of your information • Do not keep "just in case it might be useful one day!" • Check your organisation's disposal policy • Dispose of your information correctly Retention guidelines and schedules for retentions for types of processing can be found at the following link: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016
6) Personal data be processed in a secure manner	**Take practical steps to ensure information is kept confidential.** • Ensure security of confidential faxes by using Safe Haven/Secure faxes – but fax should be used as a last resort to other secure methods of transmission such as NHS mail, encryption etc. • ALWAYS keep confidential papers locked away when not in use • Consider working practices and if areas are accessible by the public/ external staff then consider whether clear desk policy is appropriate • Ensure confidential conversations cannot be overheard • Keep your password secret • Ensure information is transported securely – local procedures should be developed and made available to staff if this is a requirement of the role.
7) Accountability	**Demonstrate compliance** • Ensure all data processing activities are documented. • Handle personal data lawfully, fairly and securely. • Only access information when required for your role. • Use approved systems and secure methods for storing and sharing data.

Attachment 2- Breakdown of the NHS statutory lawful bases for processing data.

Legislation/Statutory Duty	Purpose/scope	Article 6 legal basis	Article 9 Special category
Abortion Act 1967 and Abortion Regulations 1991	Requires that health and care staff share information with the Chief Medical Officer about abortion treatment they have provided.	6(1)(e) public task	Article 6(1)(e) – Public task / official authority
Access to Health Records Act 1990	Allows access the health records of deceased people, for example to personal representatives or those who have a claim following the deceased person's death.	6(1)(e) public task	Article 6(1)(e) – Public task / official authority
Health and social Care Act 2008	Regulation of health and social care services: quality and safety duties, CQC requirements.	6(1)(c) Legal obligation or 6(1)(e) public task	9(2)(h) Health and social care
NHS Act 2006 (as amended)	NHS Functions, commissioning, care provision, information sharing for care.	6(1)(e) public task	9(2)(h) Health and social care
Health and social Care Act 2012	Duty to share for care: public health functions, commissioning	6(1)(e) public task	9(2)(h) Health and social care or 9(2)(i) public health

Care Act 2014	Adult safeguarding duties care assessments	6(1)(c) legal obligation or 6(1)(d) vital interests	9(2) Substantial public interest or 9(2)(h)
Coroners and Justice Act 2009	Sets out that health and care organisations must pass on information to coroners in England.	6(1)(c) legal obligation	Article 9(2)(g) – Substantial public interest
Children's act 1989/2004	Child safeguarding: duty to share risks of harm	6(1)(c) legal obligation or 6(1) (d) vital interests	9(2) Substantial public interest
Control of Patient Information Regulations 2002 (COPI)	Allows information to be shared for specific reasons in relation to health and care, such as for the detection and prevention of cancer, to manage infectious diseases, such measles or COVID-19. It also allows for information to be shared where support has been given for research or by the Secretary of State for Health and Social Care.	6(1)(c) legal obligation	9(2)(i) Substantial public interest
Fraud Act 2006	Defines fraudulent activities and how information may be shared, for example with the police, to prevent and detect fraud.	Article 6(1)(c) – Legal obligation	Article 6(1)(e) – Public task (exercise of official authority)

Public Health (Control of disease) Act 1984	Disease control, notification, infection management	6(1)(c) legal obligation	9(2)(i) public health
Human Fertilisation and Embryology Act 1990	Requires health organisations to report information about assisted reproduction and fertility treatments to the Human Fertilisation and Embryology Authority.	Article 6(1)(c) - Legal obligation	Article 6(1)(e) - Public task / exercise of official authority
Health Protection (Notification) regulations 2010	Mandatory reporting of notification, infection management.	6(1)(c) legal obligation	9(2)(i) public health
Human Tissue Act 2004	Requires health organisations to report information about assisted reproduction and fertility treatments to the Human Fertilisation and Embryology Authority.	Article 6(1)(c) – Legal obligation	Article 6(1)(e) – Public task / official authority
Employment Rights Act 1996 & working time regs	HR, employment records, pay, training, workforce management.	6(1)(b) Contract or 6(1)(c) legal obligation	9(2)(b) Employment
Equality Act 2010	Equality monitoring and reporting	6(1)(c) legal obligation	Article 6(1)(e) – Public task / official authority
Safeguarding Vulnerable Groups Act 2006	Sets out requirements for organisations who work with vulnerable to share information and to perform pre-employment checks with the Disclosure and Barring Service (DBS), which is responsible for helping employers make safer recruitment decisions.	Article 6(1)(c) - Legal obligation	Article 6(1)(e)- Public task / official authority

Attachment 3- **Consent form examples**

Consent to Process Personal Data

We will use your personal data to provide XXXXX our services and carry out our functions. This may include collecting, recording, storing, and using your information in accordance with data protection law.

What this means for you

We will:

- Use your personal data **lawfully, fairly and transparently**
- Only collect data that is **necessary for the stated purpose**
- Keep your information **accurate and up to date**
- Store your data **securely** and only for as long as needed
- Not use your data for incompatible purposes without informing you
-

Your rights

You have the right to:

- Request **access** to your personal data
- Request **correction** of inaccurate information
- Request **erasure or restriction** of processing (where applicable)
- **Object** to certain types of processing
- Withdraw your consent at any time (where consent is the legal basis)

Further details about how we use your information and how to exercise your rights can be found in our privacy notice:
[insert privacy notice link]

Consent statement

☐ I confirm that I have read and understood how my personal data will be used and I **consent to its processing** for the purposes described above.

Consent to Take Part in Health Research and Use of Personal Data
Use of your information in this research

We will need to use information from you and/or your medical records for this research project. This information is sometimes called personal data. It may include special category data, such as health information.

We will:

- Use your information only for the purposes of this research
- Handle your data in accordance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Ensure your information is kept confidential, secure, and only accessible to authorised staff
- Remove your name and identifiers wherever possible and replace them with a study ID number (pseudonymisation)

The organisation responsible for this study (the data controller) is:
[Insert NHS organisation / sponsor name]

Sharing your information

Your information may be shared with:

- Authorised researchers working on this study
- Regulatory authorities (e.g. MHRA, HRA) to check the study is conducted properly
- NHS organisations involved in your care

Where possible, shared data will not directly identify you. We will not share your identifiable information with third parties for purposes unrelated to this research without your consent, unless required by law.

How long we keep your data

We will keep your information for **[insert retention period, e.g. 5–25 years depending on study type]** in line with NHS and research governance requirements.

Your choices and rights

Taking part in this study is completely voluntary.

You can:

- Withdraw from the study at any time, without giving a reason
- Ask for access to the information we hold about you
- Ask for your data to be corrected if it is inaccurate

If you withdraw:

- We will stop collecting new information about you
- Information already collected may still be used to ensure the integrity and reliability of the research

Legal basis for using your data

We are using your data because:

- It is necessary for a task carried out in the public interest (scientific research)
- We are processing special category data for scientific research purposes with appropriate safeguards
- Your consent to take part in the study is separate from the legal basis we use to process your data.

Further information

You can find out more about how we use your data in our privacy notice:
[Insert link]

If you have concerns, you can contact:

[Data Protection Officer contact details]
The Information Commissioner's Office (ICO): www.ico.org.uk

Consent Statement

Please initial/tick each box:

☐ I have read and understood the information sheet for this study

☐ I understand how my personal data will be collected, used and shared

☐ I understand that my participation is voluntary and I can withdraw at any time

☐ I agree to take part in this research study

Name (Participant): _____

Signature: _____

Date: _____

Attachment 4 - **Template fair processing notice <ENTER SERVICE NAME>**

<DESCRIPTION OF THE SERVICE – what is the service about?>

http://www.royalwolverhampton.nhs.uk/patients-and-visitors/privacy-ico/#

What information do we collect about you?	List the types of data and the format, e.g. paper records, clinical system, images, CCTV, audio recordings etc.
How do we use this and what is the legal basis?	Describe the uses of the data you collect. If for direct care then this will be similar to the Trust notice but also consider other (secondary) uses such as planning, reporting, research etc. and what legal basis supports this. If anonymised data will be used for secondary purposes, then state this. If relying on consent to process and not a legal basis, this is where you state this. Always select a legal basis is there is one over consent. Breakdown of the NHS statutory lawful bases for processing data can be found in attachment 2.
Who do we share your information with?	Detail the recipients (who you share the data with) whether this is a one off or routine.
Who and where do we obtain your information from?	If this is directly from the individual state the ways in which data is collected. If this is from other sources or organisations detail this.

What rights do I have in relation to my information?

Below is a list of the rights you have in relation to your data and when they apply. To make an application for any of the below rights please contact the Health Records Access Team rrwh-tr.healthrecordsaccess@nhs.net in the first instance. All rights should be considered within 30 calendar days from date of receipt but may be extended if complex.

Please read the IG policy for details on which rights will apply to your service. Right of access will always apply- example below include:

The Right to Be Informed
You have the right to know how the NHS uses your personal data, why it is collected, how long it is kept, and who it is shared with. The Right of Access
You have the right to request a copy of any information held by the Trust as well as any supplementary information. See How do I request my information? for details on how to request your information.

How do I request my information?

The Right to Rectification
If your information is incorrect or incomplete, you can ask for it to be corrected.

The Right to Restrict Processing
You can ask the NHS to stop using your data in certain situations—e.g., while accuracy is being checked.

The Right to Object
-Processing is based on public interest or legitimate interests
-Some objections may not apply if there is a strong legal basis for NHS processing.

Rights Related to Automated Decision-Making and Profiling

- Not to be subject to decisions made solely by automated means that significantly affect you
- To request human review of such decisions.

How long is my information kept for?

All our records are destroyed in accordance with the NHS Retention Schedule, which sets out the appropriate length of time each type of NHS records is retained. We do not keep your records for longer than necessary.

All records are destroyed confidentially once their retention period has been met, and the Trust has made the decision that the records are no longer required. For more information please see the Record Management Code for Practice for Health and Social Care 2016, retention schedules.

You must state the retention that is applicable to the service from this guidance.

How to make a complaint

If you have any questions about your care or a complaint, please speak to the health professional with your care in the first instance. If this is not resolved to your satisfaction you can contact the Patient Advice and Liaison Service (PALS). If you have any concerns about how your information is being processed or any of the rights as detailed above, please contact the Trust in the first instance through:

Email: rwh-tr.dpo@nhs.net

You also have a right to complain directly to the Information Commissioner's Office if you feel the Trust has not responded effectively to any of the above.

Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF Telephone: 0303 123 1113

Data Protection Impact Assessment (DPIA)

Section 1 What is a DPIA and what should it include?

It is a requirement of the UK General Data Protection Regulations that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

The UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 make privacy-by-design a key legal requirement, under the term 'data protection by design and by default'.

The UK GDPR mandates the completion of Data Protection Impact Assessments (DPIA). An effective DPIA will help to ensure that potential data protection and privacy issues and risks are identified at an early stage. This will improve compliance with data protection and privacy laws and standards and uphold the rights and freedoms of living individuals. This formal assessment must be completed from the start of implementing a new system, project, or change.

The Data Protection Impact Assessment (DPIA) is a tool which helps assess data protection and privacy risks to individuals in the collection, use and disclosure of information.

The core principles of conducting a DPIA can be applied to any project, initiative, system or process change which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

Please note, a DPIA is a living document. Therefore, once a DPIA has been completed and signed off, it is recommended that it is reviewed when any changes are made to the project, initiative, system or process change to ensure that the DPIA is still accurate.

A project which has included a DPIA at the very start of the project, and updated as the project progresses should result in the project being less privacy intrusive and therefore less likely to affect individuals in a negative way.

As part of completing a DPIA, the flow mapping of data must be recorded. Any risks identified by completing the DPIA must be entered onto the relevant organisation's suitable risk register.

To support you with completing this DPIA template, you may wish to contact your Data security and protection team who may be able to provide copies of completed DPIAs for similar projects. This may be helpful to set out the level of information that is required when completing a DPIA.

Please note, Appendix A provides a list of key definitions which may be helpful to refer to.

Table of Contents

Contents

Section 1 What is a DPIA and what should it include? 1

Section 2 – Project outline and Screening Questions 3

Section 3 Project Details 6

Section 4 Describe the data 7

Section 5 Which organisations are involved and Flows 13

Section 6 Data Retention 14

Section 7 Information Assets 17

Section 8 Data Privacy Rights 18

Section 9 – Technical Support Documentation 21

Section 10 Business Continuity Planning 21

Section 11 Stakeholder Consultation 22

Section 12 What data protection risks are there and what mitigations will you put in place? 1

Appendix A: Definitions and Glossary 3

Document Review Control Information

Version	Date	Reviewer Name(s) and Job title	Change/amendment

Section 2 – Project outline and Screening Questions	
Division and Directorate	
Project Name	
Project outline i.e. This will be a description of the project proposal, this will outline the proposed changes and highlight the potential benefits of the change.	
Is this for a replacement of a current system/device	☐ Yes ☐ No
Cross reference to other/previous projects/systems/DPIAs/Replacements - add details i.e. Please provide details of the cross references such as DPIA reference/name, name of the systems etc	
Is this project in relation to a medical device?	☐ Yes ☐ No **If Yes please provide the certificate of conformity and its UKCA/CE mark, in addition please make contact with Medical Physics and Clinical Engineering to make them aware of the device:** rwh-tr.mpce-cis@nhs.net

The RWT Author completing this assessment	
Name	
Job Title	
Email Address	
Connection to Project i.e. Project manager	

Screening questions	Yes/No
1. Will you be using new technology to process personal data? ***i.e. This may include a new piece of medical equipment/system, a new application, undertaking a research study.***	
2. Are you using existing technology? If yes, are you processing personal data in a new way.	
3. Does the technology involve the processing of personal data that might be perceived as being privacy intrusive? **'Intrusive' would refer to something that disrupts, interferes with or imposes on an individual in an unwelcome or excessive way. Examples would include:** - **Monitoring (**Monitoring relates to a general approach to observation and recording of activities within a system.) - **Tracking (**Tracking would refer to gathering data relating to an individual's movement, path of specific events. Data tracking, in a data protection context, involves collecting and analyzing data about an individual's activities, behaviours, and preferences. This can include tracking online activity, location, purchases, or other personal data**)** - **Profiling (**Profiling analyses aspects of an individual's personality, behaviour, interests and habits to make predictions or decisions about them.**)** - **CCTV, facial recognition, use of biometrics* such as thumb prints, Vehicle number plate recognition or location tracking.**	
4. Does the initiative involve the processing of personal identifiable data which will then be subject to anonymisation or pseudonymisation? **Anonymisation refers to the process of turning personal data into anonymous information so that a person is no longer identifiable.** **Pseudonymisation relates to techniques that replace, remove or transform information that identifies a person and store it separately. For example, replacing one or more identifiers which are easily attributed to people (such as names) with a pseudonym (such as a reference number).**	

5. Does the project process special category data on a large scale. Some personal data is deemed more sensitive [special category] and is therefore subject to further protection. Please see list below (this is not exhaustive): - 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; - biometric data (where used for identification purposes); - data concerning health;	
6. Does the project involve the linking of personal data from multiple sources?	
7. Is personal data shared externally i.e to an external organisation or Third Party?	
8. Does any phase of the initiative use automated decision making when processing personal data? **[Automated decision-making is a decision made by automated means without any human involvement (e.g. online credit checks)]**	
9. Does your project involve the use of Artificial intelligence for the processing of personal data? **If you answer 'yes' to this question please complete the below AI DPIA Template.** DPIA Template 2025 AI Version.docx	

10. Will the processing involve individuals who are considered 'vulnerable' i.e. children, persons with disabilities?	

If any of the screening questions have been answered "YES", then please continue with the full Data Protection Impact Assessment Questionnaire (below the screening). If all questions are "NO", please return the document to the Information Governance Team and **do not** complete the full Data Protection Impact Assessment.

Please email the completed screening to the data security and protection team:

rwh-tr.ig-enquiries@nhs.net

Section 3 Project Details	
1. What is the purpose of the project/service and what are the benefits of using or sharing the data?	
2. **Supplier** If you are using a supplier please provide the name of the supplier	
3. **Proposed go live date**	
4. **Are there any data controllers? If so please provide the details of all controllers and joint controllers** For further details on this please refer to Question 36	
5. **Are there any data processors? If yes please provide the details of all data processors** For further details on this please refer to Question 36	
6. **Has a DTAC been completed? (Digital Technology Assessment Criteria)**	Yes ☐ Please Provide a copy No ☐

Section 4 Describe the data	
7. Is the data identifiable?	**[Put an ☒ next to all that apply.]** ☐ Personal data [individuals can be identified] ☐ Pseudonymised data [identifiers, for example name or NHS number, are replaced with a unique number or code (a pseudonym) ***[Provide details of any pseudonymised data, including which organisation holds the key that allows the data to be re-identified.*** ☐ Anonymous data [not identifiable, for example trends or statistics]- ***Describe the way the data has been anonymised and whether it is anonymised in the hands of those you will be sending it to. This should include detail of whether the data has been aggregated with small numbers suppressed. For example, if only two people in the area have a rare condition it could be possible to identify them so this data would need to be removed.***
8. If you have selected Pseudonymised or Anonymous data, will the data be linked with any other data sets that could result in the data becoming identifiable.	

9. Please use the data dictionary to help identify the data items you will be using and input these in the below columns for the data subjects you are processing data about:

Data Dictionar v2.docx

Select the Data Subjects identified in the data dictionary	
Patients	☐
Staff	☐
Carers	☐
Public	☐
Visitors	☐
Other: Provide details	

10. Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?

Data protection laws mean that organisations must identify which law they are relying on when sharing information. For example if an organisation is sharing information because they are required by law to do so, they need to identify which law is requiring this.
[The list below contains the most likely conditions applicable to health and care services. Put an ☒ next to the one that applies. If a different lawful basis applies for a different party, clearly indicate which lawful basis applies to which party by adding in brackets after the selected lawful basis which party it applies to e.g.

☐	**(a) We have consent** *[this must be freely given, specific, informed and unambiguous. It is not appropriate to rely on consent for individual care or research, even if you have obtained consent for other reasons, but is likely to be needed for the use of cookies on a website]*
☐	**(b) We have a contractual obligation** *['For the performance of a contract to which the 'individual' is a party']*
☐	**(c) We have a legal obligation** *[the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See this list for the most likely laws that apply when using and sharing information in health and care.]*
☐	**(d) the processing is necessary in order to protect the vital interests of the data subjects or of another natural person** *[the processing is necessary to protect someone's life]*
☐	**(e) the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.** *[a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities. See this list for the most likely laws that apply when using and sharing information in health and care. This is mostly likely to be relevant for the provision of NHS and social care services regulated by the CQC. See HRA guidance on legal basis for processing data for research]*
☐	**(f) We have a legitimate interest**

	[for example, a private care provider making attempts to resolve an outstanding debt for one of its service users. This cannot be relied on by public bodies in the performance of their tasks.]
☐	**Other** *[please state]*

11. If you have identified in question 9 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?

[The list below contains the most likely conditions applicable to health and care services. Put an ☒ next to the one that applies.]

☐	**(a) We have consent** *[this must be freely given, specific, informed and unambiguous. It is not appropriate to rely on consent for individual care or research, even if you have obtained consent for other reasons, but is likely to be needed for the use of cookies on a website]*
☐	**(b) We need it to comply with our legal obligations for employment is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment.** *[for example, to check a person's eligibility to work in the NHS or a local authority. See this list for the most likely laws that apply when using and sharing information in health and care.]*
☐	**(c) the processing is necessary in order to protect the vital interests of the data subjects or of another natural person** *[the processing is necessary to protect someone's life]*
☐	**(d) We have a legal obligation** *[the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See this list for the most likely laws that apply when using and sharing information in health and care.]*
☐	**(e) We need it to perform a public task** *[Processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.]*

☐	**(f) We need it for legal claims, to seek legal advice or judicial acts** *[the information is required to exercise, enforce or defend a legal right or claim, for example a person bringing litigation against a health or care organisation.]*
☐	**(g) We need to comply with our legal obligations to provide information where there is a substantial public interest, as set out in this list** *[for example, safeguarding of children and individuals at risk.]*
☐	**(h) We need it to comply with our legal obligations to provide or manage health or social care services** *[providing health and care to a person, or ensuring health and care systems function to enable care to be provided. See this list for the most likely laws that apply when using and sharing information in health and care.]*
☐	**(i) We need it to comply with our legal obligations for public health** *[using and sharing information is necessary to deal with threats to public health, or to take action in response to a public health emergency (such as a vaccination programme). See this list for the most likely laws that apply when using and sharing information in health and care.]*
☐	**(j) We need it for archiving, research and statistics where this is in the public interest** *[for example, health and care research, with relevant safeguards in place for the use of the participant's health and care information. See this list for the most likely laws that apply when using and sharing information in health and care. See HRA guidance on legal basis for processing data for research. Processing must be in the public interest to rely on this lawful basis.]*
☐	**Other** *[please state]*
☐	**Not applicable** *[the use of special category data is not proposed]*

12. What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?

[The common law duty of confidentiality says that health and care information about a person cannot be disclosed without that person's consent. Implied consent can be used when sharing relevant information with those who are directly involved in providing care to an individual. Explicit consent is normally required for purposes beyond individual care unless one of the other conditions set out below applies, for example you have section 251 support.]

[Put an ☒ next to the one that applies.]

☐	Implied consent
☐	Explicit consent *[a very clear and specific statement of consent]*
☐	Section 251 support *[this means you have support from the Secretary of State for Health and Care or the HRA following an application to the Confidentiality Advisory Group (CAG). CAG must be satisfied that it isn't possible or practical to seek consent.*
☐	Legal requirement *[this includes where NHS England has directed an organisation to share the data using its legal powers. State the legal requirement in the further information section.*
☐	Overriding public interest *[for example to prevent or detect a serious crime or to prevent serious harm to another person. The justification to disclose must be balanced against the public interest in maintaining public confidence in health and care services. Routine use of this is extremely rare in health and care, as it usually applies to individual cases where decisions are made to share data.*
☐	Not applicable

13. Please provide further information or evidence.

[Provide evidence as follows depending on your selection in question 13]

- A record of the explicit consent is stored in ….
- The CAG reference number is…

[for research the DPIA should cover multiple projects, so signpost to the sponsor's list of research projects with relevant CAG reference numbers]

- The legal requirement is…

[for example directed by NHS England under the Health and Social Care Act 2012]

- The overriding public interest justification we are relying upon is…

Section 5 Which organisations are involved and Flows

14. List all the organisations involved on the below table:

Controllers decide the why and how the data is being used and shared

Processors are being instructed by the controller how to use and share the data

Organisation Name	Are they a Controller/Joint Controller/Processor	ICO Registration Number	Are they compliant with the Data Security and Protection Toolkit

15. List any organisations that have been subcontracted by your **processor** to handle data

[Your processor can only sub-contract an activity to another organisation with your authorisation. The organisation which has been sub-contracted is known as a sub-processor.

Where sub-processors are not being used, state not applicable.]

16. Ask the processor what assurances are in place for the sub-processors:

17. Please describe where the data will come from and go to, these are called data flows.

i.e. ***[This may be directly from the individuals or from a third party, such as another health and care organisation.***

[You can use this table - some examples have been provided. Alternatively, you can use a data flow map or a written description of the data flow. A simple example of a map could be: patient - inputs blood pressure reading into app X - reading uploaded into patient's hospital record.]

Remove example below when completing your flow.

Data flow name	Going from (Source organisation and include its storage method Example RWT Amazon Web Services)	Method of transfer and frequency	Going to (Destination organisation and include their storage method)	Data description

18. Are you storing information?

[Put an ☒ next to the one that applies.]

☐ Yes [go to question 19]
☐ No [skip to question 20]

19. How will the information be stored?

If this is offsite with a third party please provide further details of how they will store the information.

20. Will any data be shared outside of the UK?

[Put an ☒ next to the one that applies.]

☐	Yes [go to question 21]
☐	No [skip to question 23]

21. If yes, give details, including locations and any safeguards or measures put in place to protect the data whilst outside of the UK.

i.e [An example of a safeguard is an up to date international data transfer agreement (IDTA). This should be included in your contract with the overseas organisation. For countries without UK adequacy in place, further checks on the organisation must be made before providing them access to data to ensure the data will be handled appropriately.]

22. How will you ensure clear instruction has been given for the use of the data?

(examples: Contracts/Data sharing agreements/Data Processing Agreements/SOPs)

23. How will you monitor the ongoing use and access of the data in line with the above?

Explain what you will do and how often
(Example: Audits, Site visits, contract monitoring)

Section 6 Data Retention

24. How long will RWT keep the data for?

You intend to start using the data on [add date] and will finish using the data on [add the contract/project/programme end date or indicate if it is ongoing]

25. How long will the supplier/processor keep the data for?

This should be stipulated in any contracts or processing agreements.

26. What will happen to the data at the end of this period?
[Put an ☒ next to all that apply.]

Action		The Royal Wolverhampton NHS Trust Details	The supplier/Processor if applicable
☐	Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction) ***[provide details of who will do this]***		
☐	Permanent preservation by transferring the data to a Place of Deposit run by the National Archives ***[provide details of who will do this]***		
☐	Transfer to another organisation ***[provide details]***		
☐	Extension to retention period ***[with approved justification]***		
☐	It will be anonymised and kept ***[provide details of how this will be done and by who]***		
☐	The controller(s) will manage as it is held by them		
☐	Other ***[please state. For research, explain the exemptions applicable to research. Explain the safeguards as set out in HRA guidance on safeguards]***		

Section 7 Information Assets

27. Is this project using an existing Information Asset

[Your service will have an Information Asset Owner and Administrators that are trained to log Information Assets, the IG team can support you in identifying these key individuals: Information Asset Management]

[Put an ☒ next to the one that applies.]

☐	Yes – Please provide the One Trust information asset reference
☐	No [go to question 28]

28. If no please confirm that you have registered the new Information Asset and its reference:

☐	Yes – Please provide the One Trust information asset reference:
☐	No – provide the reason why

29. Who is the information asset owner:

Section 8 Data Privacy Rights

30. **How will you comply with the following individual rights (where they apply)?**

Individual right	**How you will comply (or state not applicable if the right does not apply)**
The right to be informed **The right to be informed about the collection and use of personal data.** ***[Put an ☒ next to all that apply.]*** The right to be informed is part of the GDPR's transparency requirements. The minimum requirements for the right to be informed under the General Data Protection Regulation (GDPR) include: • Providing clear and concise information about how personal data is collected and used • Making the information available in a precise, transparent, and easily accessible form • Providing information in writing or electronic for	
The right of access – How will data subjects be able to request a copy of their data? This is commonly referred to as a subject access request.	

The right to rectification – How will data subjects be able to action their right to rectification? The right to have inaccurate personal data rectified or completed if it is incomplete.	
The right to erasure – How will data subjects be able to action their right to erasure if applicable The right to have personal data erased, if applicable. *[This will not apply if you have selected the following as your legal basis as legal obligation, public task or legal claims, or if you have selected health and care services, public health or archiving, research or statistical purposes]*	
The right to restrict processing – How will data subjects be able to action their right to restricted processing? The right to limit how their data is used, if applicable. *[For example, that it can be held by the organisation, but restrictions placed on how it is used. This is unlikely to apply to health and care organisations.]*	
The right to data portability The right to obtain and re-use their personal data, if applicable. *[This only applies where you are processing under UK GDPR consent, or for the performance of a contract; and you are carrying out the processing by automated means, therefore excluding paper files.]*	

The right to object – how will data subjects be able to action their right to object? The right to object to the use and sharing of personal data, if applicable. ***[This applies where you are carrying out a task in the public interest or for your legitimate interests, but there are exceptions. It is unlikely that an objection would be upheld where the data is processed for individual care, but each request must be considered on a case-by-case basis. However, it is important to note that there are other routes in which an individual can raise an objection to processing.]***	

31. **Will the national data opt-out need to be applied?**

[Put an ☒ next to the one that applies.]

☐	Yes *[provide details of how this is applied]*
☐	No *[provide details of why this is not applicable]*

[The national data opt-out applies to the use of confidential patient information for purposes beyond individual care, for planning and research. It will only apply if your answer to Q12 is that you require section 251 support, although there are some exceptions in which it would not apply to programmes with section 251 support.]

32. Will any decisions be made in a purely automated way without any human involvement (automated decision making)?

Automated decision-making is the process of making a decision by automated means without any human involvement.

[Put an ☒ next to the one that applies.]

☐ Yes

☐ No

Section 9 – Technical Support Documentation

33. Complete the Technical Support Documentation.

Please note the supplier/processor may be able to assist you with these questions.

If this is internal processing please seek the assistant of your specialist IT services.

☐ Completed

Technical Support Questions.docx

Section 10 Business Continuity Planning

34. Do you have a business continuity plan in place to cover this processing?

35. In the event of an outage how do you communicate this to your users?

36. In the event of an outage with a third party, what is their response time with communication to their users?

37. How do third parties ensure business continuity is covered for data processing activities?

38. How are the business continuity plans tested?

39. Are there service level agreements (SLAs) addressing continuity and data protection?

☐ Yes

☐ No

40. If Yes how are these enforced in the event of a disruption?

41. How Would disruptions affect critical business processes?

42. How business critical is the system you are using – tick only one:
☐ Tier 1– Critical (restoration asap within 24 hrs)
☐ Tier 2 – Significant (restoration within 24-48 hrs)
☐ Tier 3 – Moderate (restoration within 1week)
☐ Tier 4 – Minor (restoration over 1week)

43. How would business continuity plans be tested?

Section 11 Stakeholder Consultation

44. Detail any stakeholder consultation that has taken place (if applicable).

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security.

For research, you should include information about the sponsors policies and procedures for public involvement in research, and additional specific involvement relating to use of confidential patient information without consent under section 251 support.]

Section 12 What data protection risks are there and what mitigations will you put in place?

45. Complete the risk assessment table below:

You must consider risks at each stage, for example when data is being transferred, when it is stored and when it is no longer needed. Consider whether there are any responses to questions in this DPIA that are either inconclusive or insufficient.

Use the Risk Assessment Matrix to calculate the risk scoring based on likelihood and impact.

Risk Ref no	**Description of the risk**	**Risk Score*** **(L x I)**	**Mitigations** What is being put in place to reduce the risk	**Risk Score with mitigation's applied** **(L x I)**	**IG Comments**	**Categorisations of risk** (to be completed by IG)

Risk Assessment Matrix

The risk matrix is a tool used in a Data Protection Impact Assessment (DPIA) to assess the likelihood and severity of risks to individuals' rights and freedoms. The matrix helps to quantify the risk and establish criteria for accepting risks.

Likelihood represents the probability of that event occurring.

Impact reflects the potential impact the risk event will have on an individual.

		Impact (I)				
		Negligible (1)	Low (2)	Moderate (3)	Significant (4)	Catastrophic (5)
Likelihood (L)	Rare (1)	1	2	3	4	5
	Unlikely (2)	2	4	6	8	10
	Possible (3)	3	6	9	12	15
	Likely (4)	4	8	12	16	20
	Almost certain (5)	5	10	15	20	25

Appendix A: Definitions and Glossary

Definitions

DPIA	Data Protection Impact Assessment
UK GDPR	UK General Data Protection Regulations
ICO	Information Commissioners Office
DPO	Data Protection Officer

Glossary

Anonymisation

Anonymisation is the process of rendering data into a form which does not identify individuals, and where identification is not likely to take place. By definition, anonymised data do not relate to a particular individual any more than they relate to anyone else in the underlying population.

Biometric data

'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (finger print) data;

Business sensitive data

"Business sensitive" relates to information and documentation which is created, that requires confidentiality due to the legal, ethical or commercial content. Information that, if disclosed, could prejudice, or cause reputational or financial damage to an organisation.

Consent

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Cyber Essentials
A government accredited set of basic technical controls to help organisations protect themselves against common online security threats. The scheme enables organisations to gain one or two Cyber Essential badges and is suitable for organisations of any size, in any sector https://www.cyberessentials.ncsc.gov.uk/

Data portability
'The right to data portability allows individuals to obtain and reuse their personal data 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 affecting its usability'.

Genetic data
'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

ISO 27001
ISO 27001 is the international standard that provides specification for best-practice information security management systems (ISMS). It provides a certificated accreditation and is supported by a code of practice for information security management.

Lawful basis for processing
The lawful bases for processing are set out in Article 6 of the General Data Protection Regulations. At least one of the lawful basis for processing must apply whenever you process personal data. (see appendix B for a full list).

Personal data
"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;

Pseudonymisation

Pseudonymisation is 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.

Special categories of data

Special categories of data are considered as more sensitive data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Information Governance Investigation Root Cause Analysis Report

This report is to be completed when the information governance incident has been scored as a 2 or above, following the IG calculator document. To be completed by the Investigating officer or their nominee and attached this report to Datix.

Please note that any emails or other documents prepared in connection with this incident must be added as documentation onto Datix. Circulation of such documents must be restricted to those directly involved in investigating the incident. Please do not reference any data subjects by name in this report.

***DSP Team use only* - Has the incident been externally reported?

Information Commissioners Office (ICO)	
DSP Toolkit Ref:	
Police Ref:	
Other:	

RCA investigator - Name /job role	
Date of investigation	
Datix Number	
Date of incident	
Time of Incident	
Location of Incident (internal or external)	
Details of any persons and regulatory bodies who have/may need to be informed	
Caldicott Guardian	Provide date
Senior Information Risk Owner	Provide date
Data subjects	Provide date and name
Other	Provide date and details
Number of Data Subjects affected	
Any sensitive data involved – children's, Safeguarding etc.	
Volume of records involved	
Has the data been recovered?	

1.0 Details of incident. Assessment of any related policies, procedures or guidance which have been breached or wider issues *[provide copies of any local guidelines or procedures which have not been followed]*

2.0 Detail what immediate actions were taken to mitigate against any risk or harm to data subjects(s).
1. 2. 3.

Full Investigation - RCA report

1.0 Timeline of Events/Chronology

Date/time	Event	Source/s of evidence

2.0 Contributory Factors

Contributory findings/ factors make the event more likely or the harm more severe, and so play a part in **causing or influencing the incident.** Even if they are not the root cause and don't have a clear solution they must be recorded below. Authors must aim to identify any 'Human Factors' involved. Where Human factors, human error or behavioural influences are identified please be sure to complete the error classification and behavioural influences below to ensure there is appropriate understanding is the affecting issues and for action planning. (Incidental findings or observations can be recorded under lessons learnt and shared learning where these are relevant to improve outcomes or reduce recurrence).

Individual (e.g. physical, psychological, social, personality issues, fatigue, stress, hunger, anger/ frustration)	
Team & Social (e.g. role congruence, leadership, support and cultural factors including whether it was an ad hoc team or formed team, whether there a was a brief/ debrief) Communication (e.g. verbal, written, non-verbal	
Communication (e.g. verbal, written, non-verbal communication).	
Task (e.g. guidelines, procedures, policies, decision making aids)	
Education and training (e.g competence, supervision, availability and appropriateness.)	
Equipment & Resource (e.g. displays, integrity, positioning, usability, availability, 'making-do', standardisation)	
Working Conditions (e.g. administrative, physical environment, staging, workload, time pressure (real or perceived)	
Organisational/Strategic (e.g. organisational structure, priorities, safety culture, any learning from previous similar incidents / near miss?)	
Patient (e.g. clinical condition, mental / psychological, physical, interpersonal)	
Technology issues Any vulnerabilities in networks, systems, or software are identified	

3.0 Identifying the Root Cause

Why did it happen? (Root Causes identified using '5 whys')
i.e what were the underlying factors that led to this IG incident. Please describe how these factors led to this incident. 1. 2. 3. 4. 5.
How will the root causes be addressed?
1. 2. 3. 5.
Lessons learnt and shared learning for the wider team/ Trust
Advise of any general learning from this IG incident that have been identified. The below lessons should be considered.
Attachments or evidence to support investigation
i.e please attach any information that has been gathered as part of the incident.

4.0 Data Subject Impact

Has the Data Subject been informed? If not is there a plan to do this?
What was the impact/harm/distress for the Data Subjects(s)

5.0 Action plan template

No	Root Cause	Recommendation to address identified root cause/s and human factors	Action/s to implement recommendation	Implementation lead (Job Title)	Target Date for completion	Evidence for completed action
1						
2						
3						

The Royal Wolverhampton NHS
NHS Trust

IG Audit Checklist Pre meet

information governance
Handling information with confidence

Division/ Directorate:	
Department/Ward:	
Pre Meet Undertaken by:	
Date of Pre Meet	

Pre Audit: DEPARTMENT/ SERVICE PRACTICE CHECKLIST

The following practices should be checked with the service lead to understand process and practice.

Section 1: Staff awareness (DSPT Standards E, A1, B6)		**YES**	**NO**	**N/A**	**NOTES**
1.0	Are staff made aware of any local procedures and practices in relation to information governance and confidentiality practices? If yes how do you make staff aware? - *as a part of their induction or in team briefings?*				
1.2	How are service users/ patients told of how their information is used? - *Privacy notices*				
1.3	Are all staff compliant with their Information Governance mandatory training on My Academy?				

	What's your process for managing where staff have expired IG mandatory training?				
1.4	Are Staff aware of individual rights and if so would they know where to direct a request such as a Subject Access Request - *Health Records for SAR* - HR for staff				
1.5	The Service understands what a DPIA is and when its required? *What is a DPIA?* *When would it be required*				
1.6	Staff understand what constitutes as an Unauthorised Access? Do they know how to report an allegation of unauthorised access? Do you know how to request an audit log activity? How long would you request the audit log to cover?				
Section 2: Data flows and transfers (DSPT Standards A3 and B3)					
2.0	Staff do not send personal information via email other than from NHS.net addresses to NHS.net addresses or equivalent? - *Where this might be happening is secure email options are being used?*				
2.1	If a patient or service user objects to sharing or processing of their data, there is a process for managing this? *Information Governance* *Health Records – rights request*				
2.2	Before sharing identifiable information are there options or restrictions that are considered? *Consent* *Opt Out*				

Section 3: Security (DSPT Standard B2)					
3.0	Does your area have a record of ownership of mobile devices is up to date and devices can be tracked using logs and these are being used properly and kept up to date.				
3.1	Do you review staff system permissions following disciplinary action or if a staff member is subject to investigation of unauthorised access which has been founded as illegitimate access?				
Section 4: Access Control (DSPT Standard B2)					
4.0	Do individual staff members have access rights appropriate to their role for access to data or systems containing personal and sensitive data of patients/staff				
4.1	Where users no longer require access to the system, how do you ensure their rights have been revoked? *leavers process how is this followed*				
4.2	Privileged access: do you continuously review staff members with elevated access rights and ensuring they still have a legitimate business need?				
4.3	Are generic accounts in use and if so what for? Do you have a log of these accounts				
4.3.1	How are passwords and access managed and monitored and has this been risk assessed?				
Section 5: Business continuity (DSPT Standard B3)					
5.0	In the event of any disruptions to systems can you evidence data availability and recovery in the department business continuity plans *Do they have the business continuity plan?*				
5.1	When was your business continuity plan last tested?				

5.2	Is there evidence of learning following previous business continuity.				

IG Audit Staff Knowledge Check & Observational Check

information governance
Handling information with confidence

Division/ Directorate:	
Department/Ward:	
Audit Undertaken by:	
Date Audit Completed	

PART 1 - STAFF KNOWLEDGE CHECK During the Audit

These questions are to be asked to a selection of staff from the service in order to test staff understanding at all levels.

Staff Awareness (DSPT Standard B6)		**YES**	**NO**	**N/A**	**NOTES**
1.0	Do you know where to find relevant Information Governance policies, for example • IG Policy (OP13) and the purpose of the policy • Trust's confidentiality code of conduct and the purpose of the Code (OP97). *Where?*				
2.0	Who is the Trust's: Caldicott/ SIRO/ DPO				
3.0	Do you understand what constitutes as an Unauthorised Access? Do you know how to report an allegation of unauthorised access?				

4.0	Do you understand and know the rules about who you can share personal data with and how. *E.g Consent/confirming identity/secure email*				
5.0	If you are working off-site or at home do know not to remove patient identifiable information from the Trust				
6.0	Can you provide an example of what constitutes as an IG incident (see OP10) *Ask for an example*				
7.0	Where are the procedures located for managing different types of IG incidents and how to report on Datix				
8.0	Are staff devices secured when out of the office/ off site? *Do you leave Laptops in cars* *iPads devices in the home.*				
Compliance with access control (DSPT Standard B6)					
9.0	Do you understand data access procedures when accessing trust systems *e.g. not using the user name/password issued to them/ writing down passwords etc*				
10.0	Are you aware that your activities on IT systems are monitored and recorded?				
11.0	You do not use your own personal devices to store/ process patient data? *Including images*				

Security (DSPT Standard B6)					
12.0	Are you aware of what to do if you receive a suspicious email or link? *What do you?*				
12.0	Do you know you shouldn't use the same password for multiple systems and why this is important? *Cyber awareness training*				
13	Have you completed your Cyber awareness training				
Patient Communication and Preferences (DSPT Standard E)					
14.0	Where would you direct patients/ or employees if they want to request a copy of their personal data (OP07/ HR09)				
15.0	Where would you direct anyone wanting to make a Freedom of Information request (OP90)				

PART 2 - OBSERVATIONAL CHECK

The following practices should be observed in person to understand working practices

	Safe Haven & Confidentiality Practices	YES	NO	N/A	NOTES
1.0	Is personal information being moved from desks/ ward receptions/ patient areas to the secure area as soon as practical?	☐	☐	☐	
2.0	Are patient records being stored securely when not in use?	☐	☐	☐	
3.0	Where identifiable information is being sent by post, evidence that envelopes are sealed, marked 'confidential' and to a named recipient. Are addresses being checked for accuracy?	☐	☐	☐	
4.0	Is patient waste which includes personal information (e.g. waste medicine boxes with labels) being put into the controlled waste bin as soon as practically possible or alternatively labels shredded as required by the Trust procedures?	☐	☐	☐	
5.0	Did the bins contain any patient or other identifiable information?	☐	☐	☐	
6.0	Was sensitive conversations regarding service users overheard?	☐	☐	☐	
7.0	When identifiable information is being disclosed, are staff reminded to check that it all relates to the correct individual?	☐	☐	☐	
8.0	Confirmed that where identifiable information is sent via email, staff are checking recipient before sending, and attachments are password protected where possible.	☐	☐	☐	
9.0	When providing information over the telephone was it witnessed that the callers identify was confirmed?	☐	☐	☐	
10.0	Are records accessible by unauthorised personnel?	☐	☐	☐	
11.0	**Security Measures**				
12.0	Is the department secured against unauthorised access. Are there controls to prevent tailgating/ swipe access to get to areas where data is held/ stored?	☐	☐	☐	

13.0	Confirmed that windows and doors are being locked each evening as per the security arrangements	☐	☐	☐	
14.0	Are computers shut down when not in use/ locked when unattended?	☐	☐	☐	
15.0	Is IT equipment locked down to prevent theft?	☐	☐	☐	
16.0	Confirmed that where generic accounts are in use, confidential information not saved to desktop.	☐	☐	☐	
17.0	Confirmed that passwords are not written down/ on display	☐	☐	☐	
18.0	Are all staff wearing and displaying Trust ID badges?	☐	☐	☐	
19.0	Are there any USB sticks or other external storage left plugged in?	☐	☐	☐	
20.0	Are desks kept clear of confidential information?	☐	☐	☐	
21.0	Are lockable cabinets available?	☐	☐	☐	
22.0	Are keys secured?	☐	☐	☐	
23.0	Blue bins available for confidential waste	☐	☐	☐	
24.0	Are the RA cards removed from the PC when not in use?	☐	☐	☐	
25.0	Are portable devices secured when not in use?	☐	☐	☐	

Actions/ Recommendations :	Date

Information Governance Review & Feedback (if appropriate) Sign Off					
Name:				Date:	
Grade your result:	*Review the return and grade and provide rationale if different*		Significant gaps to address	Minor concerns to address	No issues identified
Additional comments:					

Attachment 8 - Template communication for Notification to individuals regarding an incident

Dear **[Recipient Name],**

Data breach Incident

We are writing to inform you of a data protection incident at **[The Royal Wolverhampton NHS Trust]** involving some of your personal information. We are sorry to tell you that your personal information has/may have been included in this data breach.

We understand the importance of handling your data safely, and we are contacting you to explain what happened, what information was involved, and the steps we are taking to put things right.

Details of the incident:

On **[date]**, we identified that e.g. [**Information was sent to the wrong recipient / documents were misplaced / an administrative error occurred / data was accessed in error].** This incident was caused by e.g. **[System error],** and we took immediate action to contain the situation.

Based on our investigation, the following personal information may have been affected:

Examples below:

- Name
- Address
- Date of birth
- NHS number
- Health information — specify type if applicable

We took immediate steps to reduce any risk and to prevent recurrence, including:

- E.g. Completed a root cause analysis.
- E.g. Implemented a new process.

At this stage, we do not believe you are at direct risk because of the incident. However, we want you to be aware so you can contact us if you notice anything unusual or have any concerns.

We sincerely apologise for this incident and any concern it may cause. Protecting your personal data is extremely important to us, and we are taking all appropriate steps to improve and maintain the security of your information.