NHS
Yorkshire
Ambulance Service
NHS Trust

Data Protection Policy

Author: Head of Risk & Assurance and Data Protection Officer (DPO)

Approved: February 2025

Document Reference	PO – Data Protection Policy – February 2028
Version	V10.0
Responsible Director (title)	Director of Corporate Services and Company Secretary, Deputy Chief Executive
Document Author (title)	Head of Risk & Assurance and Data Protection Officer (DPO)
Approved by	Information Governance Working Group
Date Approved	February 2025
Review Date	February 2028
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal and Public Website

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
1.0	March 2007	David Johnson	A	Initial version produced.
2.0	April 2010	David Johnson	A	Minor amendments including addition of new process for disclosure.
3.0	March 2012	David Johnson	A	Inclusion of a section relating to the security of hard copy data taken off site.
4.0	6 Nov 2013	Caroline Squires	A	Approved TMG
5.0	Nov 2015	Caroline Squires	A	Approved by TMG
6.0	May 2018	Risk Team	A	Approved at TMG
7.0	May 2021	Risk Team	A	Approved at TMG
8.0	June 2021	Risk Team	A	Appendix A amended – Q31 changed and formatting completed
8.1	February 2023	Head of Risk and Assurance	D	Full review Surveillance Camera Systems Policy quoted Visitors to YAS Premises Policy quoted 3.10.5 – amended name of assurance group from Quality Committee to RAG 6.3 – As above Appendix C – Risk & Assurance Group added – Quality Committee removed GDPR replaced with UK GDPR
9.0	April 2023	Risk Team	A	Approved at TMG
9.1	January 2025	Head of Risk & Assurance and DPO	D	Full review Responsible Committee amended Responsible Director Amended Document Author title amended 6.3 – wording amended from Bi monthly & 10 security standards to current wording Appendix C – Roles & Responsibilities amended – SIRO – amended to correct director RAG info amended TMG removed Courts & Evidence policy quoted in associated documentation 3.8.3 added to section 3
10.0	Feb 2025	Risk Team	A	Policy approved at IGWG and published.
A = Approved D = Draft				
Document Author = Head of Risk & Assurance and DPO				
Associated Documentation: Insert names of associated Policies or Procedures here				

Information Governance Framework
Information Sharing Policy
Records Management Policy
Data Quality Policy
Disclosure Policy
Freedom of Information Policy
ICT Security Policy and Associated Procedures
Email Policy
Internet Policy and Procedure
Social Media Policy
Safety and Security Policy
Incident and Serious Incident Management Policy
Surveillance Camera Systems Policy
Visitors to YAS Premises Policy
Safeguarding Policy
Disciplinary Policy and Procedure
YAS Code of Conduct
Courts and Evidence Policy

Section	Contents	Page No.
	Staff Summary	6
1.0	Introduction	7
2.0	Purpose/Scope	7
3.0	Process	8
4.0	Training Expectations for Staff	17
5.0	Implementation Plan	17
6.0	Monitoring compliance with this Policy	17
7.0	Appendices	
	Appendix A – The Caldicott Principles	18
	Appendix B - Definitions	19
	Appendix C - Roles & Responsibilities	20
	Appendix D – Data Protection Impact Assessment Procedure	22
	Appendix E – Data Protection Impact Assessment	24

Staff Summary

Yorkshire Ambulance Service NHS Trust ('the Trust') is committed to protecting the rights and privacy of individuals (this includes patients, staff and others) in accordance with the General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 to which it is subject to as a data controller and processor of personal data and special categories of data.
NHS organisations are required to comply with the Caldicott Principles, Confidentiality: NHS Code of Practice and additional guidance issued by the Department of Health, Information Governance Alliance and other professional bodies.
Failure to comply with the requirements of the UK GDPR, Data Protection Act 2018 and the Common Law Duty of Confidentiality may result in Yorkshire Ambulance Service NHS Trust facing prosecution, including enforcement action, a financial penalty and disciplinary action being taken against individuals by the Trust and the relevant Professional Body (where applicable).
The Trust must have a valid legal basis in order to process personal data; these are set out in Article 6 of the UK GDPR. At least one of these must apply whenever personal data is processed.
An individual's right to be informed under the UK GDPR (Article 13 and 14) requires organisations to provide people with information about their legal basis for processing. These details are included in the Trust's privacy notice: https://www.yas.nhs.uk/tc/privacy-policy/.
To process special category data, both an Article 6 legal basis for processing must be identified and a special category condition for processing in compliance with UK GDPR Article 9.
Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right.
The UK GDPR (Article 30) obligates written documentation and overview of procedures by which personal data is processed. Records of Processing Activity (ROPA) must include significant information about data processing, including the purpose of the processing, the categories of personal data, the categories of recipients, the lawful basis for processing the personal data, and the retention period for the personal data.
When sharing personal information the Trust will ensure that the principles of the UK GDPR, the Data Protection Act 2018, the Caldicott Principles, the Common Law Duty of Confidentiality and the Human Rights Act 1998 are upheld.
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the Trust.

1.0 Introduction

1.1 Yorkshire Ambulance Service NHS Trust ('the Trust') is committed to protecting the rights and privacy of individuals (this includes patients, staff and others) in accordance with the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 to which it is subject to as a data controller and processor of personal data and special categories of data.

1.2 The Trust has a requirement to process personal data and special categories of data about its staff, its patients and other individuals for legitimate reasons in the discharge of its everyday business, for example in the provision of healthcare, to recruit and pay staff, to monitor performance and comply with legal obligations. Information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully, in order to comply with the UK GDPR and Data Protection Act 2018.

1.3 All staff additionally have a duty of confidentiality to patients under common law and also statute law which imposes legal obligations regarding confidentiality of patient identifiable data. NHS organisations are required to comply with the Caldicott Principles (see Appendix A), Confidentiality: NHS Code of Practice and additional guidance issued by the Department of Health, Information Governance Alliance and other professional bodies.

2.0 Purpose/Scope

2.1 The purpose of this policy and associated procedures is to support staff by describing the Trust's commitment to, and principles for, ensuring that personal data and special categories of data are processed in a lawful and appropriate manner.

2.2 The scope of this policy and associated procedures cover the processing of personal data and special categories of data relating to:

- Patient/client/service user information;
- Staff information;
- Personal information relating to others.

2.3 The policy and associated procedures apply to everyone working or acting on behalf of Yorkshire Ambulance Service NHS Trust including all permanent and temporary staff, contractors, students and researchers. Any individual who has authorised access to personal data and special categories of data will be expected to have read and to comply with this policy in addition to having signed up to binding clauses relating to confidentiality and data protection within an appropriate contract (or on occasions a confidentiality agreement) with Yorkshire Ambulance Service NHS Trust. It is the responsibility of Information Asset Owners to ensure a suitable contract (or agreement) is in place.

2.4 Failure to comply with the requirements of the UK GDPR, Data Protection Act 2018 and the Common Law Duty of Confidentiality may result in Yorkshire Ambulance Service NHS Trust facing prosecution, including enforcement action, a

financial penalty and disciplinary action being taken against individuals by the Trust and the relevant Professional Body (where applicable).

3.0 Process

3.1 Data Protection Principles

3.1.1 The UK GDPR sets out seven key principles which lie at the heart of the general data protection regime. UK GDPR requires personal data to be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

3.1.2 The accountability principle requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. Organisations must have appropriate measures and records in place to be able to demonstrate their compliance.

3.2 Data Subjects Rights

3.2.1 The UK GDPR provides the following rights for individuals:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

3.2.2 The Disclosure Policy provides further information on individual's rights.

3.3 Legal bases for processing under the UK GDPR

3.3.1 The Trust must have a valid legal basis in order to process personal data; these are set out in Article 6 of the UK GDPR. At least one of these must apply whenever personal data is processed.

3.3.2 There are six available legal bases for processing:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: 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.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3.3.3 The first data protection principle requires that all personal data is processed lawfully, fairly and in a transparent manner. If no legal basis applies to the processing, it will be unlawful and in breach of the first principle.

3.3.4 An individual's right to be informed under the UK GDPR (Article 13 and 14) requires organisations to provide people with information about their legal basis for processing. These details are included in the Trust's privacy notice: https://www.yas.nhs.uk/tc/privacy-policy/.

3.3.5 The legal basis for processing can also affect which rights are available to individuals.

3.3.6 To process special category data (see Appendix B - Definitions), both an Article 6 legal basis for processing must be identified and a special category condition for processing in compliance with UK GDPR Article 9.

3.3.7 The conditions for processing special category data are:

(a) Explicit consent;
(b) Employment, social security and social protection (if authorised by law);
(c) Vital interests;
(d) Not-for-profit bodies;
(e) Made public by the data subject;
(f) Legal claims or judicial acts;
(g) Reasons of substantial public interest (with a basis in law);
(h) Health or social care (with a basis in law);
(i) Public health (with a basis in law);
(j) Archiving, research and statistics (with a basis in law).

3.3.8 To process personal data about criminal convictions or offences, both a legal basis under Article 6 and legal authority or official authority for the processing must be identified under Article 10 of the UK GDPR.

3.4 Consent and Fair Processing

3.4.1 Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options.

3.4.2 Under UK GDPR Ambulance Trusts are classified as public authorities and therefore the use of the 'legitimate interests' justification is not possible in terms of the Trust's core activities (public tasks). It may be possible to use legitimate interests for processing that is undertaken outside of the Trust's public task.

3.4.3 The Trust will ensure that patients are informed if their decisions about disclosure have implications for the provision of care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

3.4.4 Public authorities should not use consent as the legal basis of processing personal data for their core activities due to the imbalance in the relationship between the data controller and the data subject. In these cases it is unlikely that consent could be deemed to be freely given. Therefore, the Trust will clearly identify alternative legal justifications for processing, in accordance with Article 6 of the UK GDPR (see 3.3.2 above).

3.4.5 Where patients have been informed of the use and disclosure of their information associated with their healthcare and the choices that they have and the implications of choosing to limit how information may be used or shared, then consent is not the appropriate legal basis for information disclosures needed to provide that healthcare.

3.4.6 Where the purpose is not directly concerned with the healthcare of a patient however, consent may be the appropriate condition for processing. The Trust will ensure that additional efforts to gain consent that is informed and freely given are made and any consent is recorded or that alternative approaches that do not rely on identifiable information are developed.

3.4.7 In the situations where consent for the use or disclosure of patient identifiable information is not the appropriate legal basis, and where the public good of this use outweighs issues of privacy and the Common Law Duty of Confidentiality, Section 251 of the NHS Act 2006 provides a statutory power to ensure that NHS patient identifiable information needed to support essential NHS activity can be used without the consent of patients. Under these scenarios the appropriate conditions for processing will be either Article 6(1)(c) processing is necessary for compliance with a legal obligation, or Article 6(1)(e) processing is necessary for the performance of the public task. The Health Research Authority receive and may approve applications under Section 251 of the NHS Act 2006.

3.4.8 Seeking the consent of patients, where this is the appropriate legal basis, may be difficult due to illness, disabilities or circumstances that may prevent them from comprehending the likely uses of their information. The Mental Capacity Act (2005) is intended to protect people who lack the capacity to make their own decisions. The Act allows the person, while they are still able, to appoint someone (for example a trusted relative or friend) to make decisions on their behalf, in their best interest, for their health and personal welfare, once they lose the ability to do so. The Act introduces a Code of Practice for healthcare workers who support people who have lost the capacity to make their own decisions. The Trust will ensure it complies with the Code of Practice in relation to patients who lack capacity and where consent is used as the condition for processing.

3.4.9 In order to promote a healthcare service which is open and transparent about how patient information is used and processed the Trust will ensure information is made available to patients about how their information will be collected, stored, used and shared with partner organisations for the provision of continued healthcare. See https://www.yas.nhs.uk/tc/privacy-policy/.

3.4.10 The Trust will also notify staff of the reasons why their information is required, how it will be used and to whom it may be disclosed. In most instances the legal basis to

process personal and sensitive data will not be consent but is more likely to be Article 6(1)(b) processing is necessary in the performance of a contract, Article 6(1)(c) processing is necessary for compliance with a legal obligation, or Article 6(1)(e) processing is necessary for the performance of the public task. The appropriate condition for processing will be clearly identified in the Trust's Records of Processing Activity (ROPA).

3.5 Records of Processing Activity (ROPA)

3.5.6 The UK GDPR (Article 30) obligates written documentation and overview of procedures by which personal data is processed. Records of Processing Activity (ROPA) must include significant information about data processing, including the purpose of the processing, the categories of personal data, the categories of recipients, the lawful basis for processing the personal data, and the retention period for the personal data.

3.5.7 The Trust is required to make the ROPA available to the ICO, as the supervisory authority, on request so that it can demonstrate compliance with its obligations under UK GDPR.

3.5.8 Failure to maintain records of processing activity constitutes an offence under the UK GDPR and could result in the Trust receiving a fine of up to 10 million euros or 2% of annual turnover.

3.6 Information Sharing

3.6.1 When sharing personal information the Trust will ensure that the principles of the UK GDPR, the Data Protection Act 2018, the Caldicott Principles, the Common Law Duty of Confidentiality and the Human Rights Act 1998 are upheld.

3.6.2 The Trust is currently a signatory to a number of information sharing agreements which provide the basis for facilitating the lawful exchange of personal data between health and other partner organisations.

3.6.3 See the Information Sharing Policy for further details.

3.7 Research

3.7.1 The Trust will ensure that personal data collected for the purposes of research is processed in compliance with the UK GDPR and Data Protection Act 2018.

3.7.2 Personal data processed for research purposes only, receives certain exemptions from the UK GDPR and Data Protection Act 2018 if:

- The data are not processed to support measures or decisions with respect to particular individuals and;
- If data subjects are not caused substantial harm or distress by the processing of the data.

If the above conditions are met the following exemptions may be applied to personal data processed for research purposes only:

- Personal data can be processed for purposes other than that for which they were originally obtained (exemption from Principle B)
- Personal data can be held indefinitely (exemption from Principle D)
- Personal data are exempt from data subject access rights where the data are processed for research purposes and the results are anonymised.

3.7.3 Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes, the Trust expects that wherever possible, researchers will contact participants if it is intended to use data for purposes other than that for which they were originally collected.

3.7.4 Researchers must adhere to the Trust's Records Management Policy, although it is recognised that the Act allows personal data processed only for research purposes to be kept indefinitely.

3.7.5 Researchers must ensure that the findings of research are anonymised when published and that no information is published that would allow individuals to be identified without the explicit consent of the data subject.

3.8 Anonymisation and Managing Data Protection Risk

3.8.1 Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. Fewer legal restrictions apply to anonymised data. Anonymisation is of particular relevance, given the increased amount of information being made publicly available through the Government's Open Data agenda. The Protection of Freedoms Act 2012 enhances access to information by requiring a public authority to consider data held in a dataset that is not already published. Where the Freedom of Information Act 2000 requires the publication of a dataset the Trust is required to release it in a form that is reusable.

3.8.2 The Trust will ensure that data released under the Freedom of Information Act 2000 and the Government's Open Data agenda are fully anonymised. All staff will adhere to the Information Commissioner's 'Anonymisation Code of Practice' which describes the steps an organisation must take to ensure that anonymisation is conducted effectively, while retaining useful data.

3.8.3 Further information regarding the Freedom of Information Act 2000 can be found in the Freedom of Information Policy.

3.9 Information Security of Personal and Confidential Data Including Data in Transit

3.9.1 The Trust will ensure that policies and procedures are in place to enable compliance with Principle F of the UK GDPR. This principle requires that "appropriate technical or organisational measures" must be taken in the protection of personal data and special categories of data.

3.9.2 All staff must adhere to basic principles for preventing theft, fraud, and confidentiality and security breaches e.g. locking the door to a secure area and not leaving ID cards on desks. All staff must:

- Adhere to this policy and it's supporting procedures and guidance;
- Ensure security practices are observed and carried out as part of their daily routine;
- Wear ID badges at all times;
- Query the status of strangers if safe to do so;
- Inform their line manager if anything suspicious or worrying is noted;
- (When working from home) consider the environment and others in the home to ensure that confidentiality is maintained. Examples of adaptations may include using headsets rather than speakers, or changing the position of the monitor screen to prevent it being viewed by others in the home.

3.9.3 In addition, in order to achieve robust information security and to protect the Trust's information assets all staff must:

- Comply with the UK GDPR and Data Protection Act 2018, Common Law Duty of Confidentiality, Caldicott Principles and Confidentiality: NHS Code of Practice;
- Ensure premises and vehicles are suitably secure so as not to put information assets, e.g. laptops or paper records containing confidential data, at risk;
- Ensure they only use and share confidential data that they are authorised to use and share, with organisations or individuals that are authorised to receive it;
- Ensure information published to online and digital sources is fully anonymised and does not breach the UK GDPR and Data Protection Act 2018;
- Ensure that when anonymised or pseudonymised information is shared care is taken to ensure that the method used to anonymise or pseudonymise is effective and individuals cannot be identified from the limited data set, e.g. age and postcode together could be sufficient enough to reveal an individual's identity;
- Ensure all records containing confidential data are stored in secure areas with appropriate and adequate controls in place, i.e. in a lockable room with controlled access or in a locked drawer;
- Ensure Smartcards are not left unattended and cards and access PIN codes are not shared with other staff;
- Ensure computer passwords are not shared with other staff and computer workstations not left unattended and insecure;
- Ensure personal data, special categories of data and commercially sensitive data held and transported on portable devices, e.g. laptops and removable media, has been approved in advance by the Trust's Senior Information Risk Owner (SIRO) and is encrypted to 256 bit AES encryption;
- Ensure emails containing patient identifiable data, sensitive staff identifiable data or commercially sensitive information are only transmitted outside of the Trust's own secure email network if the email or email transmission method is

encrypted to 256 bit AES encryption. Refer to the Email Policy for mandated requirements;

- Ensure personal data, special categories of data and commercially sensitive data transmitted via the internet or file transfer protocol is encrypted to 256 bit AES encryption;
- Have a clear business need to use paper-based copies of documents containing personal data, special categories of data or commercially sensitive information off-site;
- Ensure that laptops, tablet computers, other portable computer devices and telecommunications equipment are secure when in transit and when used away from secure work premises;
- Ensure personal data, special categories of data or commercially sensitive data is not stored on personal computer devices. All equipment used for work purposes must be supplied by the Trust, unless staff are using the Trust's Outlook on the web server or NHSmail.

3.10 Data Breaches

3.10.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the Trust. Examples of personal data breaches might include:

- Sending an email intended for one email address to another email address in error;
- Losing hard copy records or electronic devices, which contain personal data;
- Disclosing personal data to someone without the appropriate authority.

3.10.2 Any data breaches or near misses (where a data breach was narrowly avoided) should be reported through the Trust's incident management system in line with the Incident Management Policy.

3.10.3 In certain circumstances, there is a requirement to report a data breach involving personal data to the Information Commissioner's Office (ICO) within 72 hours of a breach being discovered, therefore it is important to report the breach without undue delay.

3.10.4 If the breach is likely to result in a high risk to the rights and freedoms of the 'data subject', the incident will be reviewed by the Trust's Data Protection Officer (DPO) in line with NHS Digital's Guide to the Notification of Data Security and Protection Incidents and reported through the Data Security and Protection Toolkit (DSPT).

3.10.5 Breaches are reported to the Information Governance Working Group (IGWG), with reportable breaches escalated to the Risk and Assurance Group (RAG), which is a sub-group of the Trust Board. Breaches are also reported to the Trust's Caldicott Guardian and Senior Information Risk Owner (SIRO), who are Board members. See Appendix B for Definitions and Appendix C for Roles and Responsibilities. Reportable breaches are also reported in the Trust's Annual Governance Statement,

part of the Annual Report and Accounts, which is reported to and approved by the Trust Board.

3.11 Data Protection Impact Assessments

3.11.1 Data Protection Impact Assessments (DPIAs) are a tool recommended by the Information Commissioner's Office to build data protection compliance into projects and initiatives from their inception. A DPIA is a process to help the Trust identify and minimise the data protection risks of a project/initiative.

3.11.2 Under the UK GDPR and the Data Protection Act 2018, a DPIA should be carried out whenever any Trust project/initiative affects personal data in such a way that is likely to result in a high risk for the rights and freedoms of the individuals. Examples include: implementing new systems/databases, new projects, and new information sharing arrangements with third parties, but only where personally identifiable data is involved.

3.11.3 A DPIA should be carried out, in particular when an initiative includes:

- A systematic monitoring of a publicly accessible area on a large scale;
- A systematic and extensive evaluation of personal data which is based on automated processing, and on which decisions are based that produce legal effects concerning or significantly affecting the people involved; or
- Processing on a large scale of highly sensitive categories or data (including criminal convictions and offences).

3.11.4 The relevant Information Asset Owner (IAO) should seek the advice of the Information Governance Team when carrying out a DPIA. The Data Protection Officer (DPO) should be consulted and have final sign off on all DPIAs.

3.11.5 For any DPIA that identifies a high risk that cannot be mitigated, the DPO must consult the ICO before the processing can begin.

3.11.6 DPIAs are intended to build in "privacy by design" and are also intended to prevent privacy related problems from arising by:

- Considering the impact on privacy at the project start;
- Identifying ways of minimising any adverse impact;
- Building this into the project as it develops.

3.11.7 The Trust's Data Protection Impact Assessment Procedure can be found in Appendix D.

3.12 Data Protection Complaints and Enquiries

3.12.1 Complaints about the Trust's data protection procedures will be dealt with by the Data Protection Officer, who will deal with the complaint in accordance with the Trust's Complaints Policy.

3.12.2 General enquiries about the UK GDPR or Data Protection Act 2018 will be dealt with through the Information Governance Team.

4.0 Training Expectations for Staff

4.1 Training is delivered as specified within the Trust Training Needs Analysis (TNA).

5.0 Implementation Plan

5.1 The latest ratified version of this policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this policy and associated procedures during Trust Induction.

6.0 Monitoring Compliance with this Policy

6.1 Via the Integrated Performance Report, the Trust Board will monitor to ensure that no UK GDPR or Data Protection Act undertakings, enforcement notices, or monetary penalty notices are served on the organisation by the Information Commissioner's Office.

6.2 Data breaches will be monitored by the Caldicott Guardian and Information Governance Working Group (IGWG).

6.3 The Risk and Assurance Group (RAG) will monitor overall compliance through receipt of reports every two months in relation to the National Cyber Security Centre's Cyber Assessment Framework (CAF) aligned Data Security and Protection Toolkit (DSPT). The IGWG will monitor operational progress throughout the year and take action to address any concerns. Any deficiencies will be noted and reviewed at subsequent meetings.

7.0 Appendices

Appendix A: The Caldicott Principles

- **Principle 1 - Justify the purpose(s) for using confidential information**
  Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

- **Principle 2 - Use confidential information only when it is necessary**
  Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

- **Principle 3 – Use the minimum necessary confidential data**
  Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

- **Principle 4 - Access to confidential information should be on a strict need-to-know basis**
  Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

- **Principle 5 - Everyone with access to confidential information should be aware of their responsibilities**
  Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

- **Principle 6 - Comply with the law**
  Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

- **Principle 7 - The duty to share information for individual care is as important as the duty to protect patient confidentiality**
  Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

- **Principle 8 - Inform patients and service users about how their confidential information is used**
  A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Appendix B: Definitions

Personal Data	Personal Data is any information relating to natural persons: • who can be identified or who are identifiable, directly from the information in question; or • who can be indirectly identified from that information in combination with other information.
Special Categories of Data	Special Categories of Data is any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a person's sex life or sexual orientation.
Data Controller	The entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	An entity that processes data on behalf of, and only on the instructions of, the relevant Data Controller.
Data Subject	Any natural person whose personal data is processed by a controller or processor.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Third Party	Any individual/organisation other than the data subject, the data controller (the Trust) or its agents.
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.
Healthcare Purposes	Includes all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. Does not include research, teaching, financial audit and other management activities.
Anonymised Data	Information which does not relate to an identified or identifiable natural person.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Appendix C: Roles & Responsibilities

Chief Executive
As the accountable officer for the Trust, the Chief Executive has overall responsibility for compliance with the UK GDPR and Data Protection Act 2018. Operational responsibility for data protection is delegated to the Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and all Information Asset Owners (IAOs).

Senior Information Risk Owner (SIRO)
The Board-level SIRO, under delegated authority from the Chief Executive, oversees compliance with the Data Protection Act and is responsible for the Trust's information risk. The Trust's SIRO is the Deputy Chief Executive. The SIRO is supported by the Data Protection Officer, Information Asset Owners, and Information Governance Team.

Caldicott Guardian
The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian is responsible for providing advice within the Trust on the lawful and ethical processing of patient information. The Deputy Medical Director acts as the Trust's Caldicott Guardian who plays a key role in ensuring that the organisation satisfies the highest practicable standards for handling patient identifiable information.

Data Protection Officer (DPO)
A Data Protection Officer (DPO) is a role mandated for public bodies, for organisations carrying out regular and systematic monitoring of data subjects on a large scale, and for organisations carrying out large scale processing of special category data (e.g. health and social care) or criminal convictions data. The Head of Risk and Assurance acts as the Trust's DPO and is supported on a day to day basis by the Information Governance Team. The DPO advises the organisation on data protection matters, monitors compliance and is a point of contact on data protection for the public and the ICO.

Director of Corporate Services and Company Secretary
The Director of Corporate Services and Company Secretary on behalf of the Trust Board is responsible for the ongoing delivery of this policy/framework. He/she will provide regular reports to the Quality Committee on progress against its implementation.

Risk and Assurance Group (RAG)
This policy/framework will be overseen by the Risk and Assurance Group (RAG), chaired by the Director of Corporate Services and Company Secretary. This group will receive assurance of ongoing progress against the policy/framework.

Information Governance Team

The Information Governance Team provides day-day-day operational support to the SIRO and Caldicott Guardian and is responsible for providing general advice and guidance on data protection and the application of this policy.

Information Asset Owners (IAOs)

The SIRO is supported by a network of Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). These individuals are responsible for interpreting information governance policy, applying it on a practical level within their area of responsibility and ensuring that policies and procedures are followed by staff. They recognise actual or potential security incidents, consult with the SIRO and Caldicott Guardian in relation to incident management and ensure that ROPA are accurate and up to date.

Information Governance Working Group (IGWG)

The Information Governance Working Group (IGWG) consists of all Information Asset Owners (IAOs).

All Staff

All staff are responsible for making sure they have read and understood this policy and associated procedures and are aware of the disciplinary and legal action that could potentially be taken if this policy and associated procedures are not followed. Compliance with data protection legislation is the responsibility of all members of staff including anyone providing a service on behalf of the Trust.

Appendix D

Data Protection Impact Assessment (DPIA) Procedure with Template

Scope

This policy applies to all those with authorised access to personal data processed by the Trust irrespective of status, including employees, temporary staff, contractors, consultants and suppliers who are involved in an initiative that affects the processing of personal data and is likely to result in a high risk for the rights and freedoms of individuals.

Purpose

All employees and third parties have a duty to protect Trust data that they create, store, process or transfer. As a result of working in an ever-changing business, there is need to continually assess the potential impact of changes to people, process and technology to ensure data is protected throughout its lifecycle.

The purpose of this document is to specify and communicate to all personnel the Trust policy on assessing business changes with respect to personal data protection. This is in line with the Trust's data protection obligations.

Policy Statement

It is Trust policy to ensure that all initiatives/projects affecting personal data shall be compliant with all legal and regulatory requirements in each of the jurisdictions in which it operates.

Roles and Responsibilities

Individuals are responsible for ensuring a Data Protection Impact Assessment (DPIA) has been carried out where applicable to an initiative they are undertaking.

Information Asset Owners (IAOs)/Line Managers are directly responsible for implementing and monitoring compliance with this policy within their functional areas.

The Information Governance Team has direct responsibility for maintaining this policy and providing advice on implementation.

What is a DPIA?

A DPIA is a process which allows organisations to identify and minimise the privacy risks of their projects. "Project" covers any plan, proposal, process or system that involves personal data of customers and / or employees.

Conditions to Carry Out a DPIA

A DPIA shall be carried out whenever any YAS initiative affects personal data in such a way that is likely to result in a high risk for the rights and freedoms of the individuals. Examples include: implementing new systems/databases, new projects and new sharing arrangements with third parties (including those providing a service for YAS), but only where personal data is involved.

A DPIA shall be carried out, in particular when an initiative includes:

- A systematic monitoring of a publicly assessable area on a large scale;
- A systematic and extensive evaluation of personal data which is based on automated processing, and on which decisions are based that produce legal effects concerning or significantly affecting the people involved; or
- Processing on a large scale of highly sensitive categories of data (including criminal convictions and offences).

The DPIA shall be carried out prior to starting the initiative.

Please refer to the DPIA Screening Questionnaire in **(Appendix A)**, which will tell you whether a DPIA **(Appendix B)** is required.

Contents of a DPIA

The assessment shall contain at least:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the interest pursued by the Trust;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks and impact to the rights and freedoms of data subjects involved; and
- The required measures envisaged to manage the risks (including owners and timescales); including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with UK GDPR.

The project manager/information asset owner (IAO) shall seek the advice of the Information Governance Team, when carrying out a DPIA.

Where appropriate, the Trust shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

Actions Following a DPIA

Where necessary, the Trust shall carry out a review to assess if the processing of personal data is being performed in compliance with the DPIA. This will be done at least when there is a change of the risk represented by the processing operations.
When the DPIA indicates that the processing would result in a high risk in the absence of measures to mitigate the risk, the Trust shall consult the relevant Supervisory Authority (The Information Commissioners Office) prior to processing any personal data. In such circumstances, the following shall be provided:

- Where applicable, the respective responsibilities of YAS and its third parties involved in the processing;
- The purposes and means of the intended processing;
- The measures and safeguards in place for data protection within this initiative;
- The contact details of the DPO; and
- The DPIA.

Appendix E

Background

A data protection impact assessment (DPIA) will help you to identify and mitigate potential data protection risks to an acceptable level before using or sharing (processing) data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

- Data protection by design - privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.
- Accountability - your organisation is responsible for showing how it complies with data protection laws.
- Transparency - personal data must be used and shared in a transparent way.
- Security - adequate measures need to be in place to protect data. This can range from policies and procedures to technical security measures such as encryption of data.

DPIAs are mandatory when there is a high risk to individuals, such as when using the health and care data of a large number of people. However, health and care organisations are strongly advised to complete a DPIA when using and sharing personal data in a new or substantially changed way.

A DPIA involves a risk assessment. If a high-level risk remains after applying mitigations, then you must consult with the Information Commissioner's Office (ICO) for further advice before starting to collect, use or share the data.

A DPIA is a live document - you must update it if there are any changes to:

- the purpose - why you are proposing to use or share personal data
- the manner - how you will use or share the data
- who is involved - the organisations using and sharing personal data

Text in [square brackets and green highlight] is guidance only and should be removed for the final version.

Text in yellow highlight is sample wording and should be edited according to your local circumstances.

Data protection impact assessment (DPIA)

Data protection impact assessment (DPIA) title:	[add the name of the initiative, programme, project or process]
Information Asset Owner:	[add name and title]
DPIA reference number:	[to be added by Information Governance team following sign off]

Section 1 - Screening questions

1. Do you need to do a DPIA?

		Y/N
1	Will you be using and sharing data which needs more protections because it is sensitive (special category data)? This includes identifiable health and care data. Types of special category data are detailed in question 6.	Choose an item.
2	Will you be implementing a new technology?	Choose an item.
3	Are there high risks to the processing (for example, data is being shared outside of the UK without adequate safeguards in place)? Please contact the IG team for guidance on 'high risks.'	Choose an item.
4	Will large numbers of people be affected, for example, converting thousands of paper records into digital format. Please contact the IG team for guidance on what is classed as a large number of people.	Choose an item.

Answering 'yes' to any of these questions is an indication that a DPIA is required.

If you think there is a low risk to individuals, you do not need to complete a DPIA. However, if you feel there is a need to consider the risks further or document your reasons for not completing a DPIA, set that out here, complete questions 1a and 1b then skip to sections 10 and 11 - the other sections do not need completing. Examples of where this may apply is where the processing is not high risk because the project involves a small dataset and the data is pseudonymised with the re-identification key held separately, or only staff names and email addresses are to be used.

a. Summary of how data will be used and shared

[For example, data is collected from our services, and aggregated. We will then share the aggregated data with Company A to gain improved insights to enable us to improve service provision.]

b. Description of the data

[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)]
☐	Anonymous data [not identifiable, for example trends or statistics]

[Provide details of any pseudonymised data, including which organisation holds the key that allows the data to be re-identified.
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.
Where a DPIA is not required but you are documenting your decision and the risks, skip to section 10 and 11 – the other sections do not need completing.]

Section 2 – Why do you need the data?

2. What are the purposes for using or sharing the data?

[Give a high-level description of the purpose(s) for example, the purpose is to look at overall health of the people in our area to ensure we have the right services in the right places.

Multiple related purposes are acceptable for one DPIA, but where these are unrelated, a separate DPIA should be completed for each one.]

3. What are the benefits of using or sharing the data?

[Set out the benefits of using and sharing the data. This should cover the benefits to the individuals whose data is being used, the benefits to the organisation(s), the wider public, or other groups if applicable.

For example, installing a new telephony system will help deliver a better service to patients because they will be able to get through to the organisation faster and the organisation will also have an audit trail to ensure better management.]

Section 3 – What data do you want to use or share?

4. Can you use anonymous data for your purposes? If not, explain why?

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

☐	Yes
☐	No
☐	Unsure [try to provide an explanation of what you think]

[Anonymous data does not identify individuals, for example trends or statistics. You should use anonymous data whenever possible. This may not always be possible, for example if your intended use of data is to provide individual care
For example, we intend to use analytical tools to identify which individuals in our local population are at high risk of diabetes so that their GP can offer them early intervention treatments.]

5. Which types of personal data do you need to use and why?

[Put an ☒ next to all that apply.]

☐	Forename	☐	Physical description,	☐	Photograph / picture of

			for example height		people
☐	Surname	☐	Phone number	☐ ☐ ☐	Location data e.g. • IP address • Other [please state]
☐	Address	☐	Email address	☐	Audio recordings
☐	Postcode full	☐	GP details	☐	Video recordings
☐	Postcode partial	☐	Legal representative name (personal representative)	☐	Other [please state]
☐	Date of birth	☐	NHS number	☐	None
☐	Age	☐	National insurance number		
☐	Gender	☐	Other numerical identifier [please state]		

[State why you need this personal data and embed a description of the dataset if available.]

6. **Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?**

[Put an ☒ next to all that apply.]

Type of data		**Reason why this is needed (leave blank if not applicable)**
☐	Information relating to an individual's physical or mental health or condition, for example information from health and care records	[be specific where possible, for example diagnostic data, care plans, medication details, test results, vitals readings are needed in order to…]
☐	Biometric information in order to uniquely identify an individual, for example facial recognition	
☐	Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	
☐	Information relating to an individual's sexual life or	

	sexual orientation	
☐	Racial or ethnic origin	
☐	Political opinions	
☐	Religious or philosophical beliefs	
☐	Trade union membership	
☐	Information relating to criminal or suspected criminal offences	
☐	None of the above	

[Embed a description of the dataset if available, unless special category data is covered in your embedded description in response to question 5.]

7. Who are the individuals that can be identified from the data?

[Put an ☒ next to all that apply.]

☐	Patients or service users
☐	Carers
☐	Staff
☐	Wider workforce
☐	Visitors
☐	Members of the public
☐	Other [please state]

8. Where will your data come from?

[This may be directly from the individuals or from a third party, such as another health and care organisation. Note this should be a brief summary - full details of the data flows are covered in section 4.]

9. Will you be linking any data together?

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

☐	Yes [provide an explanation below and then go to question 9a]
☐	No [skip to question 10]
☐	Unsure [try to provide an explanation of what you think then go to question 9a]

[For example, combining data received from a local authority with data from NHS organisations. If so, provide details of why this is necessary, for example local authority data needs to be linked with data from local NHS organisations so that we can understand admissions to care homes from different organisations.]

a. Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?

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

☐	Yes [provide details below]
☐	No
☐	Unsure [try to provide details below]

[Standalone datasets may not be identifiable when all identifiers, such as NHS number, are replaced with a code. However, if you link the dataset with other data, it could become identifiable data. For example, if once linked, you could look up which code is associated with which NHS number. You will need to factor this in when you complete section 5.]

Section 4 – Where will the data flow?

10. Describe the flows of data.

[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.]

Data flow name	Going from	Going to	Data description
Admission data	Hospital	Local authority	Demographic data of patients admitted to hospital from local authority commissioned care homes
Diabetic data	Ambulance Trust	Hospital	Demographic data of patients with diabetes requiring an ambulance

11. Confirm that your organisation's information asset register (IAR), and data flow map (now combined) have been updated with the flows described above. You may need to speak to your Information Asset Owner (IAO).

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

☐	Yes
☐	No
☐	Unsure [add as a risk in section 10 with an action to find out]

[Your organisation is required to keep a record of the types of data processing it undertakes and any information assets it holds. The IAR and data flow map documents (now combined) allow you to record both of these in one register.

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

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

☐	Yes [go to question 12a]
☐	No [skip to question 13]
☐	Unsure [add as a risk in section 10 with an action to find out then skip to question 13]

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

[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.]

Section 5 – Is the intended use of the data lawful?

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

[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. ☒ e) **We need it to perform a public task** (GP practice)]

☐	(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** [between a person and a service, such

	as a service user and privately funded care home]
☐	(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.]
☐	(e) **We need it to perform a public task** [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]

14. If you have indicated in question 6 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.]

☐	(b) **We need it to comply with our legal obligations for 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.]
☐	(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** [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]

15. 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** [for individual care or local clinical or care audits. Skip to question 16]
☐	**Explicit consent** [a very clear and specific statement of consent. Go to question 15a]
☐	**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. Go to question 15a]
☐	**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. Go to question 15a]
☐	**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. Go to question 15a]
☐	**Not applicable** [you are not proposing to use identifiable health and care data. Skip to question 16]

a. Please provide further information or evidence.

[Provide evidence as follows depending on your selection in question 15]

- 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 6 – How are you keeping the data secure?

16. Are you collecting information?

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

☐	Yes [go to question 16a]
☐	No [skip to question 17]

a. How is the data being collected?

[You should describe the method for the collection, for example it is collected by a team going through records and extracting relevant information.]

17. Are you storing information?

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

☐	Yes [go to question 17a]
☐	No [skip to question 18]

a. How will information be stored?

[Put an ☒ next to all that apply.]

	Storage location	**Details (leave blank if not applicable)**
☐	Physical storage, for example filing cabinets, archive rooms etc	[provide details including whether the facility is operated by your organisation or a third party]
☐	Local organisation servers	[provide details]
☐	Cloud storage	[provide details including whether the facility is operated by your organisation or a third party]
☐	Other	[please state]

18. Are you transferring information?

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

☐	Yes [go to question 18a]
☐	No [skip to question 19]

a. How will information be transferred?

[For example, will the information be physically moved as required, sent electronically by email, or uploaded into a shared system. Provide details of security measures to ensure the transfer is secure, for example using secure email (such as NHSmail).

19. How will you ensure that information is safe and secure?

[You need to have measures in place to ensure that the data is safe and it won't be used, either on purpose or accidentally, in ways that are unlawful. The measures needed will be dependent upon, and proportionate to, the data which is being used.]
[Put an ☒ next to all that apply.]

Security measure		Details (leave blank if not applicable)
☐	Encryption	[specify the level of encryption, such as AES 256]
☐	Password protection	
☐	Role based access controls (RBAC)	[where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions)]
☐	Restricted physical access	[where access to personal data is restricted to a small number of people, such as access cards or keys to a restricted area]
☐	Business continuity plans	
☐	Security policies	[embed these]
☐	Other	[please state]

20. How will you ensure the information will not be used for any other purposes beyond those set out in question 2?

Specify the measures below which will be used to limit the purposes the data is used for.
[Put an ☒ next to all that apply and provide details.]

Security measure		Details (leave blank if not applicable)
☐	Contract	[a legally binding contract]
☐	Data processing agreement	[this sets out the arrangements between a controller and processor and is legally binding]
☐	Data sharing agreement	[this sets out the arrangements for sharing data between the organisations involved – it may or may not be legally binding depending on the content]
☐	Data sharing and processing agreement (DSPA)	[where appropriately completed, this is a legally binding agreement that sets out the arrangements for processing and/or sharing data, and/or joint controller arrangements]
☐	Audit	[provide details, for example there will be an audit trail of those who access health and care records, which is reviewed monthly]
☐	Staff training	
☐	Other	[please state]

Section 7 – How long are you keeping the data and what will happen to it after that time?

21. How long are you planning to use the data for?

We 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.]

22. How long do you intend to keep the data?

[The time you keep the data for may differ from the period of time you intend to use the data, for example adult health records need to be kept for a minimum of 8 years from the time they were last used. The Records Management Code of Practice sets out the retention period for health and care records. Appendix 2 of the Code also includes guidance about setting a retention period for a record not covered in the retention table of the Code.]

23. What will happen to the data at the end of this period?

[Put an ☒ next to all that apply.

Action		Details (leave blank if not 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]

[The Records Management Code of Practice provides detail about what happens once a retention period has been reached.]

Section 8 – How are people's rights and choices being met?

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

[For joint controllers, indicate anything you have agreed, such as designating one controller as a point of contact for patients and service users (data subjects).
These rights will not always apply so you should review each one to see if it applies. In particular, some rights do not apply when data is being used for research purposes. The HRA has published guidance on research exemptions.]

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.		We have assessed how we should inform individuals about the use of data for [state initiative/project/programme]. We consider the communications methods below meet this obligation because [add reasons to justify your decision] [Put an ☒ next to all that apply.]
	☐	Privacy notice(s) for all relevant organisations [provide a link or describe where it will be displayed and embed a copy]
	☐	Information leaflets
	☐	Posters
	☐	Letters
	☐	Emails
	☐	Texts
	☐	Social media campaign
	☐	DPIA published (best practice rather than requirement)
	☐	Other [please state]
	☐	Not applicable
The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.		
The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.		

The right to erasure The right to have personal data erased, if applicable. [This will not apply if you have selected legal obligation, public task or legal claims in question 13, or if you have selected health and care services, public health or archiving, research or statistical purposes in question 14.]	
The right to restrict 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 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.]	

25. 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]
☐	Unsure [add as a risk in section 10 with an action to find out]

[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 question 15 is section 251 support, although there are some exceptions in which it would not apply to programmes with section 251 support.]

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

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

☐	Yes [go to question 26a]
☐	No [skip to question 27]
☐	Unsure [add as a risk in section 10 with an action to find out]

[An example of where automated decision making may be used is staff rostering.]

a. Where the effect of the automated decision on the individual is substantial, how will you uphold an individual's right not to be subjected to a decision solely made by automated means)?

[For example, you provide people with an option to ask for a human review of the decision. If the effect on people is not legally significant, for example it will only have a minor impact upon them, state this here to confirm this right is not applicable.]

b. Are you using any special category data as part of automated decision making?

☐	Yes [we are not currently aware of any examples in health and care. If this is the case contact england.igpolicyteam@nhs.net for advice.]
☐	No

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

[For example, if your processing will have a significant impact on partner organisations or the public, you may have approached them for their views and incorporated them into the design of your data use. Include any consultation with the Information Commissioner's Office (ICO) if applicable. 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 9 – Which organisations are involved?

28. List the organisation(s) that will decide why and how the data is being used and shared (controllers).

[The organisation(s) listed here will be making the decisions for example:

- to collect the data in the first place
- what data is being collected
- what it is being used for
- who it is being collected from

The organisation(s) will also be likely to have a direct relationship with those the data is being collected from, for example patients, service users or employees.
There may be more than one organisation listed here. They may be controllers for their own data, for example care homes would usually only be controller for their own residents' information even if they were all using the same software supplier to manage their care records. In some instances, organisations may be joint controllers. For example, this may apply where organisations are using the data for the same purpose, where you share a dataset with another organisation, or where you have designed a new collection with another organisation. An example of where there may be joint controllers in some instances is shared care records, where multiple health and care organisations are contributing data for the same purpose.

In the case of research, the sponsor is the controller. See HRA guidance on controllers and research]

29. List the organisation(s) that are being instructed to use or share the data (processors).

[The organisation(s) listed here will be under instruction from those listed in question 28, for example they are likely to be told:

- what data to collect
- who to collect data from
- how the collection is legal
- the purpose for the collection
- who to share the data with

- how long to keep the data

Where processors are not being used, state not applicable.
For research, explain the sponsor's policies and procedures for managing the use of data by research sites]

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

[Your processor listed in question 29 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.]

31. Explain the relationship between the organisations set out in questions 28, 29 and 30 and what activities they do

[Describe here how it has been agreed that the organisations (controllers, processors and sub-processors) will work together. For example:

- Controller A has instructed Processor B to provide an IT system. Processor B sub-contracts the IT service desk function to sub-processor C; or
- Controllers A, B and C are controllers of their own data, which is shared between them. They all use processor D's app

Where no other organisations are used, state not applicable.]

32. What due diligence measures and checks have been carried out on any processors used?

[Put an ☒ next to all that apply. Where multiple processors are used, indicate which option applies to which processor]

Due diligence measures		Details (leave blank if not applicable)
☐	**Data Security and Protection Toolkit (DSPT) compliance**	[applicable to all organisations that have access to NHS data and systems. Use the organisation search to check the latest DSPT score for any organisation required to complete DSPT]
☐	**Registered with the Information Commissioner's Office (ICO)**	[any organisation using and sharing data should be registered - add the registration number]
☐	**Digital Technology Assessment Criteria (DTAC) assessment**	[you should ask the processor for this - see question 29]
☐	**Stated accreditations**	[for example, ISO accreditation]
☐	**Cyber Essentials or any other cyber security certification**	[you can check the National Cyber Security Centre's list of organisations that have this]
☐	**Other checks**	[please state]

Section 10 – What data protections are there and what mitigations will you put in place?

33. Complete the risk assessment table. Use the risk scoring table to decide on the risk score.

[Some examples have been added below. These should be amended and added according to your local set up.
This should include:

- Confidentiality risks - for example unauthorised or accidental disclosure of or access to personal data.
- Integrity risks - for example unauthorised or accidental alteration of personal data. Consider also how you will ensure data is accurate and up to date.
- Availability risks - for example unauthorised or accidental loss of access to, or destruction of personal data.

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.]

Risk assessment table

Risk ref no.	Description	Risk score* (L x I)	Mitigations	Risk score* with mitigations applied
01	Power outage affecting Trust servers leading to loss of availability of data	10	Backup generators kick in if main system fails	2
02	Information is stored in unrestricted network areas leading to inappropriate access to data	8	Ensure project team have dedicated network space with access restricted to team members	2
03	Data is not up to date	12	Controller A will send out daily notifications of updates	4
04				

***Risk scoring table**

	Impact (I)				
	Negligible (1)	Low	Moderate (3)	Significant (4)	Catastrophic (5)

			(2)			
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

34. Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.

Risk ref no.	Action needed	Action approver	Action owner	Due date	Status e.g. outstanding/ complete

Section 11 – Review and sign-off

This DPIA should be signed off by the relevant Information Asset Owner (IAO) and then forwarded to the Trust's Data Protection Officer (DPO) for final sign off.

IAO sign-off	
IAO name:	
IAO job title:	
Date of review:	
Comments:	

DPO sign-off

DPO name:	
DPO job title:	
Date of approval:	
Comments:	