NHS
Yorkshire
Ambulance Service
NHS Trust

Data Protection Policy

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

Approved: August 2026

Document Reference	PO – Data Protection Policy – August 2029
Version	V11.0
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	August 2026
Review Date	August 2029
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal and Public Website

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
8.0	June 2021	Risk Team	A	Appendix A amended – Q31 changed and formatting completed.
9.0	April 2023	Risk Team	A	Approved at TMG.
10.0	Feb 2025	Risk Team	A	Policy approved at IGWG and published.
10.1	June 2026	Head of Risk & Assurance and DPO	D	3.3.2 - Update to Legitimate Interests Legal Basis under the Data Use and Access (DUA) Act 2025. 3.12 - Update to expand on data protection complaints process under the new DUA Act 2025. Associated Documentation - Incident and Serious Incident Management policy amended to Incident Management Policy. Patient Feedback (Including Complaints Management) Policy added. Appendix C – SIRO updated, Caldicott Guardian updated. Appendix E – DPIA template updated to reflect NHSE template. Appendix F – New Data Protection Complaints Process Map added.
10.2	August 2026	Risk Team	D	Formatted to Trust template.
11.0	August 2026	Risk Team	A	Policy approved in August IGWG and published.

A = Approved D = Draft

Document Author = Helen Jones, Head of Risk & Assurance and DPO

Associated Documentation:

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
Social Media Policy
Safety and Security Policy
Incident Management Policy
Surveillance Camera Systems Policy
Visitors to YAS Premises Policy
Safeguarding Policy (Children Young People and Adults at Risk)
Disciplinary Policy and Procedure
YAS Code of Conduct
Coroners and Courts Policy
Patient Feedback (Including Complaints Management) Policy

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 <u>Data Protection Principles</u>

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:

- Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').
- 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').
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

- 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').
- 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').
- 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:
- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

3.2.2 The Disclosure Policy provides further information on individuals' 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:
- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- 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.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- 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.

- 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 a public authority is processing data to perform its official tasks.) For public authorities, this is only likely to apply where there is no other appropriate legal basis to apply. The Data (Use and Access) Act 2025 introduces the following recognised legitimate interests:
  - Sharing with another organisation for its public task or official functions.
  - National security, public security and defence.
  - Emergencies.
  - Detecting, investigating or preventing crime.
  - Safeguarding vulnerable individuals.

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:
- Explicit consent.
- Employment, social security and social protection (if authorised by law).
- Vital interests.
- Not-for-profit bodies.
- Made public by the data subject.
- Legal claims or judicial acts.
- Reasons of substantial public interest (with a basis in law).
- Health or social care (with a basis in law).
- Public health (with a basis in law).
- 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)

3.5.1 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.

3.5.2 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.

3.5.3 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 Guidance 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 If a data subject considers that the Trust has infringed data protection legislation because of the way their personal information has been handled, they can make a formal complaint as set out in Section 164A(1) of the Data Protection Act (DPA) 2018, amended by the Data Use and Access (DUA) Act 2025.

3.12.2 The new legislation means the Trust must:
- Give the data subject a clear way to raise a data protection complaint;
- Acknowledge the complaint within 30 days of receipt;
- Without undue delay, take appropriate steps to investigate and keep the complainant informed; and Inform the complainant of the outcome

3.12.3 Complaints about the Trust's data protection procedures will be logged within the Trust's incident management system in accordance with the Trust's Incident Management Policy and then investigated by the Trust's Data Protection Officer (DPO).

3.12.4 If the data protection complaint is from a patient and/or links in with another 4Cs process, the DPO's findings will be incorporated into a response from the Patient Relations Team in accordance with the Patient Feedback (Including Complaints Management) Policy.

3.12.5 If the data protection complaint is from a member of staff, the DPO will send their findings directly to the complainant.

3.12.6 If the data protection complaint relates to a subject access request (SAR), right of rectification request, or Police disclosure, the DPO's findings will be incorporated into a response from the Legal Services Department.

3.12.7 See Appendix F - Data Protection Complaints Process Map for further details.

3.12.8 Data protection complaints made through social media will be directed to the appropriate channel.

3.12.9 If there are any doubts about the complainant's identity, then proof of identity will be requested at the earliest opportunity.

3.12.10 If someone makes a complaint on behalf of the data subject, authorisation to act on their behalf (such as power of attorney or a signed letter of authority from the data subject) must be sought. Investigations into data protection complaints will not be carried out without the appropriate authority.

3.12.11 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). This policy will be reviewed and updated following serious information governance or cyber security incidents.

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

7.1 This policy includes the following appendices:

Appendix A: The Caldicott Principles
Appendix B: Definitions
Appendix C: Roles & Responsibilities

Appendix D: Data Protection Impact Assessment (DPIA) Procedure with Template
Appendix E: Health and care: Template data protection impact assessment (DPIA)
Appendix F: Data Protection Complaints Process Map

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 Chief Information Officer. 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 Executive Director of Quality and Chief Paramedic
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: Health and care: Template data protection impact assessment (DPIA)

Health and care:
Template data protection impact assessment (DPIA)

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 with green background is guidance text.

You can add your answers to the questions within the text boxes provided. An example is shown below. Sample wording provided here should be edited according to your local circumstances.

Write your answer here

Table of contents

Data protection impact assessment (DPIA)

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

SECTION 1 – Screening questions

Do you need to do a DPIA?

Expand to see guidance notes

☐ Yes
☐ No

Explain the answer you have chosen here

Summary of how data will be used and shared

Expand to see guidance notes

Provide a summary here

Is any of the data identifiable, pseudonymised or anonymised?

Expand to see guidance notes

Put an ☒ next to all that apply.

☐ Directly identifiable data

Expand to see guidance notes

☐ Pseudonymised data

Expand to see guidance notes

Describe the way the data has been pseudonymised and provide details of which organisation holds the key that allows the data to be re-identified.

☐ Anonymised data

Expand to see guidance notes

Describe the way the data has been anonymised

Where a DPIA is not required but you are documenting your decision and the risks, go to section 10 and 11 – the other sections do not need completing.

SECTION 2 – Why do you need the data?

What are the purposes for using or sharing the data?

Expand to see guidance notes

Type your answer here

What are the benefits of using or sharing the data?
Expand to see guidance notes

Type your answer here

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

Can you use anonymous data for your purposes? If not, explain why.
Expand to see guidance notes

Put an ☒ next to the one that applies.

☐Yes
☐ No
☐ Unsure

Explain the answer you have chosen here

Which types of personal data do you need to use and why?
Put an ☒ next to all that apply.

- ☐ Forename
- ☐ Surname
- ☐ Address
- ☐ Postcode full
- ☐ Postcode partial
- ☐ Date of birth
- ☐ Age
- ☐ Gender
- ☐ Physical description, for example height
- ☐ Phone number
- ☐ Email address
- ☐ GP details
- ☐ Legal representative name (personal representative)

☐ NHS number
☐ National insurance number
☐ Other numerical identifier

Please state

☐ Photograph / picture of people
☐ IP address
☐ Other location data

Please state

☐ Audio recordings
☐ Video recordings
☐ Other

Please state

☐ None

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

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.

☐ Information relating to an individual's physical or mental health or condition, for example information from health and care records

Expand to see guidance notes

Explain why this is needed

☐ Biometric information in order to uniquely identify an individual, for example facial recognition

Explain why this is needed

☐ Genetic data, for example details about a DNA sample taken as part of a genetic clinical service

Explain why this is needed

☐ Information relating to an individual's sexual life or sexual orientation

Explain why this is needed

☐ Racial or ethnic origin

Explain why this is needed

☐ Political opinions

Explain why this is needed

☐ Religious or philosophical beliefs

Explain why this is needed

☐ Trade union membership

Explain why this is needed

☐ Information relating to criminal or suspected criminal offences

Explain why this is needed

☐ 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.

Embed your description here

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

If you have selected 'Other', please state who this is here

Where will your data come from?
Expand to see guidance notes

Type your answer here

Will you be linking any data together?
Put an ☐ next to the one that applies.
Expand to see guidance notes

☐ Yes - provide an explanation below
☐ No - go to question 10
☐ Unsure - try to provide an explanation of what you think

Explain your answer here

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.
Expand to see guidance notes

☐ Yes
☐ No
☐ Unsure

Provide details here

SECTION 4 – Where will data flow?

Describe the flows of data.
Expand to see guidance notes

Describe the data flow, or embed a map here, or use the table below.

Example table of data flows
[Replace sample text with your own data flows]

Data flow name	Going from (source)	Going to (destination)	Data description
Admission data	Hospital electronic patient record system	Local authority social care team	Extract of admission data from patient health record: demographic data only
GP health record data	GP health record	Hospital trust	Extract of GP health record for a patient made available through the GP Connect API

Confirm that your organisation's information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.
Expand to see guidance notes

Put an ☒ next to the one that applies.
☐ Yes
☐ No
☐ Unsure - add as a risk in section 10 with an action to find out

Will any data be shared outside of the UK?
Put an ☒ next to the one that applies.

☐ Yes
☐ No - go to question 13
☐ Unsure - add as a risk in section 10 with an action to find out, then go to question 13

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

Expand to see guidance notes

Provide details here

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

Expand to see guidance notes

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

Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ (a) **We have consent**

Expand to see guidance notes

☐ (b) **We have a contractual obligation**

Expand to see guidance notes

☐ (c) **We have a legal obligation**

Expand to see guidance notes

☐ (d) **We need to protect a person's vital interests**

Expand to see guidance notes

☐ (e) **We need it to perform a public task**

Expand to see guidance notes

☐ (ea) **We have a recognised legitimate interest**

Expand to see guidance notes

Put an ☒ next to the one that applies.

The recognised legitimate interest falls under:

☐ Sharing with another organisation for its public task or official functions
☐ National security, public security and defence
☐ Emergencies
☐ Detecting, investigating or preventing crime
☐ Safeguarding vulnerable individuals

☐ (f) **We have another legitimate interest**

Expand to see guidance notes

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?

Expand to see guidance notes

Put an ☒ next to the one that applies:

☐ (a) **We have consent**

Expand to see guidance notes

☐ (b) **We need it for employment purposes**
Expand to see guidance notes

☐ (c) **We need it to protect a person's vital interests**
Expand to see guidance notes

☐ (d) **We need it for our not-for-profit organisation's activities, and it relates to our current or former members, or people who have regular contact with us**
Expand to see guidance notes

☐ (e) **The person who the data is about has made that data public**
Expand to see guidance notes

☐ (f) **We need it for legal claims, to seek legal advice or judicial acts**
Expand to see guidance notes

☐ (g) **There is a substantial public interest, as set out in this list**
Expand to see guidance notes

☐ (h) **We need it to provide or manage health or social care services**
Expand to see guidance notes

☐ (i) **We need it for public health purposes**
Expand to see guidance notes

☐ (j) **We need it for archiving, research and statistics where this is in the public interest**
Expand to see guidance notes

☐ **Not applicable**
Expand to see guidance notes

What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?
Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ **Implied consent** - go to question 16
Expand to see guidance notes

☐ **Explicit consent**
Expand to see guidance notes

☐ **Section 251 support**
Expand to see guidance notes

☐ **The law either requires or allows the data to be used and shared**
Expand to see guidance notes

☐ **Overriding public interest**
Expand to see guidance notes

☐ **Not applicable** - go to question 16
Expand to see guidance notes

Please provide further information or evidence.
Expand to see guidance notes

Provide further information

SECTION 6 – How are you keeping the data secure?

Are you storing information?
Put an ☒ next to the one that applies.

☐ Yes
☐ No - go to question 17

How will information be stored?
Expand to see guidance notes

Put an ☒ next to all that apply.

☐ Physical storage, for example filing cabinets, archive rooms etc
Expand to see guidance notes

☐ Local organisation servers
Expand to see guidance notes

☐ Third party storage
Expand to see guidance notes

☐ Other
Expand to see guidance notes

Add details to support your answer(s) here

Are you transferring information?
Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ Yes
☐ No - go to question 18

How will information be transferred?
Expand to see guidance notes

How will you ensure that information is safe and secure?
Put an ☒ next to all that apply.

Expand to see guidance notes

☐ Encryption

Specify the level of encryption, such as AES 256

☐ User identity verification and authentication
Expand to see guidance notes

Specify the measures in place, for example, multi factor authentication and provide details on how this is done

☐ Role based access controls (RBAC)
Expand to see guidance notes

Please give details of what role-based access and permissions will be set

☐ Physical controls
Expand to see guidance notes

Please give details of what physical controls will be in place

☐ Security policies
Expand to see guidance notes

Please state which policies and embed here

☐ Business continuity plans
Expand to see guidance notes

Please state or embed the relevant business continuity plans

☐ Other

Please describe the other ways in which you will ensure data is safe. Or embed any other relevant documents, such as a cyber security risk assessment, confirming who has reviewed it and the outcome.

How will you ensure the information will not be used for any other purposes beyond those set out in question 2?
Expand to see guidance notes

Put an ☒ next to all that apply and provide details.

☐ Contract
Expand to see guidance notes

Please give details

☐ Data processing agreement

Expand to see guidance notes

Please give details

☐ Data sharing agreement
Expand to see guidance notes

Please give details

☐ Data sharing and processing agreement (DSPA)
Expand to see guidance notes

Please give details

☐ Audit
Expand to see guidance notes

Please give details

☐ Staff training

Please give details

☐ Other

Please give details of the other measure(s)

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

How long are you planning to use the data for?
Expand to see guidance notes

Type your answer here

How long do you intend to keep the data?
Expand to see guidance notes

Type your answer here

What will happen to the data at the end of this period?
Expand to see guidance notes

Put an ☐ next to all that apply.

☐ Secure destruction

Provide details of how the data will be destroyed, for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction. Confirm who will manage and be accountable for this

☐ Long term preservation by transferring the data to a National Archives' approved Place of Deposit
Expand to see guidance notes

Provide details of where the data will be retained and who will be accountable for it

☐ Transfer to another organisation
Expand to see guidance notes
Consider whether the controller will change at this point. For example, a commissioning organisation may become the controller of records at the end of a contract.

Provide details of the organisation(s) it will be transferred to and who will be accountable for this

☐ Extension to retention period

Provide your approved justification for this here

☐ It will be anonymised and kept

Provide details of how it will be done and who will be accountable for this

☐ The controller(s) will manage as it is held by them

Provide details here

☐ Other
Expand to see guidance notes

Please explain what will happen to the data

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

How will you comply with the following individual rights (where they apply)?
Expand to see guidance notes

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.

☐ 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 the other way(s) in which you will comply

☐ Not applicable

Describe how the communication methods above meet your obligation to comply with the right to be informed.
Expand to see guidance notes

Add your description here.

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.

Describe the arrangements

The right to rectification
The right to have inaccurate personal data rectified or completed if it is incomplete.

Describe the arrangements

The right to erasure
The right to have personal data erased, if applicable.
Expand to see guidance notes

Describe the arrangements

The right to restrict processing
The right to limit how their data is used, if applicable.
Expand to see guidance notes

Describe the arrangements

The right to data portability
The right to obtain and re-use their personal data, if applicable.
Expand to see guidance notes

Describe the arrangements

The right to object
The right to object to the use and sharing of personal data, if applicable.
Expand to see guidance notes

Describe the arrangements

Will the national data opt-out need to be applied?
Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ Yes Please provide details of how this will be applied
☐ No
Please provide details of why this does not apply
☐ Unsure - add as a risk in section 10 with an action to find out

Will any decisions be made in a purely automated way without any meaningful human involvement (automated decision-making)?
Expand to see guidance notes

Put an ☒ next to the one that applies.

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

Please provide an explanation of how the decisions are made and who it impacts.
Expand to see guidance notes

Please provide an explanation

How will the quality of the outputs and decisions be monitored and recorded?
Expand to see guidance notes

Please state

Will the effect of the decisions on the individual be significant?
Put an ☒ next to the one that applies.
Expand to see guidance notes

☐ Yes
☐ No – go to question 26

How will you provide people with information about the decision?
Expand to see guidance notes

Provide details of how you meet this requirement, including any additional safeguards you will put in place. If you do not currently meet this requirement, add as a risk in section 10 with an action to address

How can people express their views and contest the decision?
Expand to see guidance notes
If you can only partially meet this requirement, add this as a risk in section 10 with an action to address. Provide details of why you cannot (or cannot fully) meet this requirement and confirm what has been considered, and issues identified.

Provide details of how you meet this requirement, including any additional safeguards you will put in place. If you do not currently meet this requirement, add as a risk in section 10 with an action to address

How can people ask for a human intervention in the decision?
Expand to see guidance notes

Provide details of how you meet this requirement, including any additional safeguards you will put in place. If you do not currently meet this requirement, add as a risk in section 10 with an action to address

Confirm whether the decision is:
Expand to see guidance notes

Put an ☒ next to the one that applies.

☐ Based on the individual's consent
☐ Needed for a contract with the individual
☐ Required or authorised by law (public task, legal obligation)
☐ None of the above – add as a risk in section 10 with an action to address

Provide details on what you will do to ensure that you can rely on an appropriate lawful basis to allow the automated decision making to happen, or how you will change the processing to avoid automated decision making

Are you using any special category data as part of automated decision making?
Put an ☒ next to the one that applies.

☐ Yes
☐ No – go to question 26

Confirm which of the following conditions apply to the decision:
Put an ☒ next to the one that applies.

☐ The individual has explicitly consented (can only apply if you have selected consent for question 25e)
☐ Substantial public interest is our Article 9 lawful basis
☐ None of the above – add as a risk in section 10 with an action to address

Provide details on what you will do to ensure that you can meet one of the authorised conditions to allow the automated decision making to happen, or how you will change the processing so that special category data is not used for the automated decision making

Detail any stakeholder consultation that has taken place (if applicable).
Expand to see guidance notes

Provide details here

SECTION 9 – Which organisations are involved?

List the organisation(s) that will decide why and how the data is being used and shared (controllers).
Expand to see guidance notes

Type your answer here

List the organisation(s) that are being instructed to use or share the data (processors).
Expand to see guidance notes

Type your answer here

List any organisations that have been subcontracted by your processor to handle data
Expand to see guidance notes

Type your answer here

List any organisation involved but not covered above. For example, a commissioner.

Type your answer here

Explain the relationship between the organisations set out in questions 27, 28, 29, and 30 and any other relevant organisation. Explain what activities they do
Expand to see guidance notes

Type your answer here

What due diligence measures and checks have been carried out on any processors used?
Put an ☒ next to all that apply.
Expand to see guidance notes
Where multiple processors are used, indicate which option applies to which processor.

☐ **Data Security and Protection Toolkit (DSPT) compliance**
Expand to see guidance notes

Provide the DSPT details for the organisation(s)

☐ **Registered with the Information Commissioner's Office (ICO)**
Expand to see guidance notes

Provide the ICO registration number for the organisation(s)

☐ **Digital Technology Assessment Criteria (DTAC) assessment**

Expand to see guidance notes

Provide details of the assessment

☐ **Stated accreditations**

Expand to see guidance notes

Provide details of the accreditation

☐ **Cyber Essentials or any other cyber security certification**

Expand to see guidance notes

Provide details of the certification for the organisation(s)

☐ **Other checks**

Please state here the checks you have carried out

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

Complete the risk assessment table. Use the risk scoring table to decide on the risk score.
Expand to see guidance notes

Risk assessment table

Risk ref no.	Description	Likelihood (L) score	Impact score (I)	Risk score* (L x I)	Mitigations	Risk score* with mitigations applied

***Risk scoring table**

		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

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 for example, outstanding / complete

SECTION 11 – Review and sign-off

Expand to see guidance notes

Appendix F: Data Protection Complaints Process Map