NHS
Yorkshire
Ambulance Service
NHS Trust

Data Protection Policy

Document Author: Head of Risk and Assurance

Date Approved: April 2023

Document Reference	PO – Data Protection Policy
Version	V9.0
Responsible Committee	Trust Management Group
Responsible Director (title)	Executive Director of Quality, Governance and Performance Assurance, Deputy Chief Executive
Document Author (title)	Head of Risk and Assurance
Approved By	Trust Management Group
Date Approved	01/04/2023
Review Date	30/04/2025
Equality Impact Assessed (EIA)	Yes - Screening
Protective Marking	Not protectively marked

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
4.1	April 2015	Caroline Squires	A	Amendment to include flow charts for handling Section 10 and 14 under the UK GDPR and Data Protection Act 2018, as Appendix G (approved by IG Working Group in Jan 2015) Approved by TMG 22/04/15
4.2	Oct 2015	Caroline Squires	D	Minor changes for clarity and accuracy throughout the policy and appendices. Enhancement of Appendix D, internal and external post and courier service safe haven principles.
5.0	Nov 2015	Caroline Squires	A	Approved by TMG
5.1	Sept 2017	Allan Darby	D	Extension agreed at TMG in preparedness for the launch of General Data Protection Regulations which come in to force May 2018. IG policies remain best practice up to this date.
5.2	April 2018	Risk Team	D	Document formatted – New Visual Identity
5.3	April 2018	IG Manager	D	Full review to incorporate UK GDPR requirements
5.4	April 2018	IG Working Group review	D	Review of amends and agreed. YAS visual identity applied to document
6.0	May 2018	Risk Team	A	Approved at TMG
6.1	August 2020	Ruth Parker	A	Date agreed by TMG for review date extension

6.2	Feb 2021	Head of Risk and Assurance	D	Full review
6.3	April 2021	Head of Risk and Assurance	D	Added 3.9.2 following comments at IGWG
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

A = Approved D = Draft

Document Author = Head of Risk and Assurance

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 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

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.

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.

3.9 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 and Serious 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 theRisk 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, 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 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 quarterly reports in relation to the 10 Data Security Standards of the 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 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 Executive Director of Quality, Governance and Performance Assurance. 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 Medical Director acts as the Trust's Caldicott Guardian and is supported on a day to day basis by the Deputy Medical Director 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 Corporate Affairs 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.

Associate Director of Performance Assurance and Risk
The Associate Director of Performance Assurance and Risk 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 Associate Director of Performance Assurance and Risk. This group will receive assurance of ongoing progress against the policy/framework.

Trust Management Group

The Trust Management Group, chaired by the Chief Executive, will receive policies and proposals for approval.

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

Yorkshire Ambulance Service NHS Trust

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 A

DPIA Screening Questionnaire

These questions are intended to help organisations decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA is required.

Screening Questions		**Y/N**
1	Will the project involve the collection of new information about individuals?	
2	Will the project compel individuals to provide information about themselves?	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
5	Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition	
6	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private	
8	Will the project require you to contact individuals in ways which they may find intrusive?	

Data Protection Impact Assessment

Please complete all questions with as much detail as possible at concept stage. Highlight the relevant answer in yellow. Then contact the Information Governance Team who can review and provide advice or answer queries on the data protection obligations. The DPIA will need to be signed off by the Data Protection Officer (DPO).

Section 1: General Details

Project title:	
Information Asset Owner: This is the appropriate Head of Function: Name and Title	
Objective: You can pick more than one if necessary	Existing information to be used for a different purpose New information sharing arrangement with third parties New project involving collection and processing of data New system/Database Other (please state):
Will the information sharing/protect/system contain personal identifiable information? If answer is 'No' then a DPIA is not required	Yes No If yes, who will this data relate to: Service User Staff Other (please state):
Purpose: Why is the new project, new sharing arrangement, or new system/database required?	
Necessity: What would the consequences be if the information sharing/project/ system is not progressed?	
Other related projects:	
Project Key Contact: Name and Title	

Section 2: DPIA Key Questions

	Question	Response
Data Items		
1.	**Please highlight the categories of data that are involved:** **Personal** **Special Category**	Name Phone Number Date of Birth Other (please state): Address Email Address Bank Details Ethnic Origin Religious Beliefs Genetics Health Political Opinions Trade Union membership Biometrics Sexual Orientation
2.	**Describe the information flow:** The collection, use and deletion of data should be described here. It may be useful to use a flow diagram or another way of explaining information flows	
3.	**Who will have access to the information:** You can highlight more than one. Provide an explanation.	Internal (please state sections): Council HMRC Police Data Processor NHS Voluntary Organisation Other (please state): Please explain purposes for having access to the information:
4.	**What consultation/checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or special category data for this initiative/project?**	

5.	**Is there any personal/special category data that could be disregarded without compromising the project?** Question is designed to ensure that the Service only collect/share data that is 'necessary, justified and proportionate' to meet the business or employer purposes	Yes No If yes, list then do not process that data
6.	**Does the initiative/project involve the collection of data that may be unclear or intrusive?** Are all data items clearly defined? Is there a wide range of sensitive data being included? Would it be in the reasonable expectations of the data subject?	Yes No If yes, list then do not process that data
7.	**How will the information be kept up to date and checked for accuracy and completeness?**	
8.	**How many individuals' data will be processed?**	

Purpose in Section 1 will assist in establishing the legal basis for processing. For: **Personal data an Article 6 condition needs to be met;** **Special category data an Article 6 and an Article 9 condition need to be met;** **Criminal convictions or offences data an Article 6 condition needs to be met plus authorised by law.**		
Lawfulness and Fairness		
9.	**Which Article 6 legal basis are you relying on to collect/share personal data?** https://UK GDPR-info.eu/art-6-UK GDPR/ Consent should only be used if the data subject has a real free choice; this is usually unlikely for public authorities or employer/employee relationships	Consent Contractual necessity Legal Obligation Vital interests Public task Legitimate interests Explain the rationale for relying on the condition you have chosen; where appropriate include the relevant legislation.
10.	**Which Article 9 legal basis are you relying on to collect/share special category data?** https://UK GDPR-info.eu/art-9-UK GDPR/ Consent should only be used if the data subject has a real free choice; this is usually unlikely for public authorities or employer/employee relationships but could be relevant for this type of data.	Consent Obligations in connection with employment Vital interests Legitimate activities of a not for profit body or association Information has been made public by the data subject Necessary in relation to legal rights Necessary for public functions Necessary for medical purposes Necessary for reasons of public interest in the area of public health Necessary for archiving purposes N/A Explain the rationale for relying on the condition you have chosen; where appropriate include the relevant legislation.

11.	**Which Article 10 legal basis are you relying on to collect criminal offence data?** https://UK GDPR-info.eu/art-10-UK GDPR/	Legal authorisation Official capacity N/A
12.	**If relying on consent, how will that consent/non consent be obtained and by whom?** Silence or pre-ticked boxes are not acceptable. There has to be a clear affirmative action by the data subject, such as an opt-in box	
13.	**If relying on consent, what will you do if this is withheld or withdrawn?**	
14.	**Will the consent cover all processing including any intended sharing/disclosures?** The DPO/IG Manager will use this to ensure all processing activity has a legal basis	Yes No If not, please give details:
Data Processing		
15.	**Will a third party be processing data on behalf of YAS?**	Yes No If no, please go to the Q18.

16.	**Is the third party contractor/supplier of the project registered with the information Commissioner?**	Yes No Organisation (please state): Data Protection Registration Number (please state):
17.	**Does the third party/supplier contract(s) contain all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** Ask supplier for a copy of their standard contract	Yes No
Confidentiality		
18.	**Please outline how individuals will be informed why and how their information is processed/shared.** These are known as Privacy Notices https://UK GDPR-info.eu/art-13-UK GDPR/ https://UK GDPR-info.eu/art-14-UK GDPR/	
19.	**What process is in place for rectifying/erasing or restricting access to data?** What would happen if such a request were made? Can the database or process allow you to delete, rectify or restrict?	

20.	**Will an individual be able to receive their information in a machine readable format, if requested?** This is only where the information is processed by automated means.	Yes No
21.	**Will the processing of data subject the individual(s) to a decision based solely on automated means?** This is where there is no human intervention and a system determines an outcome based on pre-programming/coding (e.g. killer questions on an online recruitment portal where the applicant is unsuccessful based on their responses.	Yes No If yes, explain the impact of the decision:
22.	**Will the processing of data be used to analyse or predict personal aspects about an individual or individuals?** Known as 'profiling'.	Yes No If yes, explain the impact of the profiling:
Engagement		
23.	**Has stakeholder engagement taken place?** Professional, Union representatives, and service users are useful to consult with or ask to give their opinion on the privacy implications of the project. You need to put yourself in individuals' shoes and envisage privacy implications.	Yes No If yes, which stakeholder and how have any issues identified by stakeholders been considered? If no, please outline any plans in the near future to seek stakeholder feedback:

Information Security		
24.	**Who will have access to the information within the system?** Please refer to roles/job titles.	
25.	**Is there a useable audit trail in place for the initiative/project?** For example, to identify who has accessed a record?	Yes No N/A If yes, please give details:
26.	**Describe where the information will be stored and how it will be accessed?** If cloud based, include details around the provider access arrangements.	
27.	**Where is the information held?**	Cloud External Server In house server Other (please state):
28.	**What training and instructions are necessary to ensure that staff know how to operate the system/process/new initiative?** Staff need to be given clear instructions on their role and use of the data. The need to be aware of the required security arrangements.	

29.	**Please indicate all methods in which information will be transferred.**	By hand Email (unsecure/personal) Fax Internet (http) Internet (https) Post (normal) Recorded Delivery Secure Email Telephone N/A Other (please state):
30.	**Does the project involve privacy enhancing technologies?** Encryption; 2 factor authentication; new forms of pseudonymisation.	Yes No If yes, please give details:
31.	**If the system is being provided by a third party who has access to the data or if the data is being processed on our behalf, what security arrangements are in place?** Obtain relevant information relating to third party accreditations and certifications.	
Privacy and Electronic Communications Regulations (PECR)		
32.	**Will the project involve the sending of unsolicited marketing messages electronically such as email, fax, telephone and text?** Please note that seeking to influence an individual is considered to be marketing.	

Records Management		
33.	**What are the retention periods for this data?**	
34.	**How will the data be destroyed when it is no longer required?** If applicable, include how third parties will destroy/return the data.	
Business Continuity		
35.	**Have requirements for business continuity been considered?** This includes the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.	Yes No If yes, please give details:
Open Data		
36.	**Will (potentially) identifiable and/or sensitive information from the project be released as Open Data (be placed in to the public domain)?**	Yes No If yes, please give details:
Data Processing Outside of the UK		
37.	**Are you transferring any personal and/or special category data to a country outside the UK?** If using a supplier for a system or a data processor, it will be necessary to identify where the information will be held. Best practice is for it to be held in the UK.	Yes No If yes, which data and to which country?

38.	**Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?**	Yes No N/A If yes, who completed the assessment?
Risks and Solutions – The outcomes from Sections 1 and 2 may have led to privacy risks being identified. Use the table to document the risks, intended solution and impact, and then update the checklist below.		
39.	**Have all risk sources been taken into account?**	Yes No
40.	**Potential impacts to the rights and freedoms of data subjects are identified, in case of events including illegitimate access, undesired modification and disappearance of data.**	Yes No
41.	**Threats that could lead to illegitimate access, undesired modification and disappearance of data are identified.**	Yes No
42.	**Measures envisaged to treat risks are determined.**	Yes No

Section 3: Risks and Solutions

Risk No.	Date Raised (Month & Year)	Privacy risks identified (outcome of Section 1 & 2)	Current Risk Owner	Original Risk			Risk Control Measures	Residual Risk		
				I (1-5)	L (1-5)	Risk Rating		I (1-5)	L (1-5)	Risk Rating
1.										
2.										
3.										
4.										
5.										
6.										

Once completed, update the Risks and Solutions section of the assessment, then go to section 4.

Section 4: Review and Approval

This Data Protection Impact Assessment should be signed off by the relevant Information Asset Owner.

Name:	
Title:	
Signed:	
Date:	

Assessment reviewed by DPO:

Name:	
Title:	
Article 6 condition checked:	☐ Yes ☐ No
Article 9 condition checked:	☐ Yes ☐ No ☐ Not applicable
Article 10 condition checked:	☐ Yes ☐ No ☐ Not applicable
Comments:	
Signed:	
Date:	