NHS
Yorkshire
Ambulance Service
NHS Trust

Data Protection Policy and Associated Procedures

Document Author: Information Governance Manager

Date Approved: May 2018

Document Reference	PO – Data Protection Policy and Associated Procedures
Version	V6.0
Responsible Committee	Trust Management Group
Responsible Director (title)	Executive Director of Quality, Governance and Performance Assurance, Deputy Chief Executive
Document Author (title)	Information Governance Manager
Approved By	Trust Management Group
Date Approved	May 2018
Review Date	May 2020
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 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 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
A = Approved D = Draft				

Document Author = Information Governance Manager
Associated Documentation: Data Protection Policy - Local Care Direct Information Governance Policy Information Governance Strategy Internet Policy and Procedure Email Policy ICT Security Policy and Associated Procedures Records Management Policy Safety and Security Policy Closed Circuit Television Policy and Code of Practice YAS Code of Conduct Social Media Policy Disciplinary Policy and Procedure Management of Online and Digital Services Procedure Freedom of Information Policy Policy for Safeguarding Children and Young People Policy for the Management of Safeguarding Vulnerable Adults Policy for the Management of Domestic Abuse Policy for the Management of Allegations of Abuse of Neglect of a Child/Vulnerable Adult against Staff

Staff Summary

Everyone working or acting on behalf of Yorkshire Ambulance Service NHS Trust, including all permanent and temporary staff, contractors, students and researchers have an individual responsibility to maintain the security of personal confidential information.
Everyone must comply with the EU General Data Protection Regulations (GDPR) and Data Protection Act 2018, Common Law Duty of Confidentiality, Caldicott Principles and Confidentiality: NHS Code of Practice.
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 GDPR and Data Protection Act 2018.
The Trust's Legal Services Department oversee all disclosures of patient identifiable data and subject access requests for staff identifiable data, health and non-health records.
All subject access requests must be directed to the Legal Services Department. On no account should a member of staff try to handle a request themselves.
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 Trust will ensure that patients are informed if their decisions about disclosure have implications for the provision of care or treatment.
All members of staff handling confidential patient and staff information, whether paper based or digital (computerised) must adhere to the safe haven principles in the handling, storage and transfer of information (see Appendix D).
Information Asset Owners must ensure that a Privacy Impact Assessment is undertaken in all instances where a new project or initiative will use personal data or special categories of data (see Appendix E).
Failure to comply with the requirements of the GDPR and Data Protection Act 2018 and 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 Yorkshire Ambulance Service NHS Trust and the relevant Professional body (where applicable).

1.0 Introduction

1.1 From 25 May 2018 the Data Protection Act 1998 has been replaced by the EU General Data Protection Regulations (GDPR) 2016 and the Data Protection Act (DPA) 2018. 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 this new EU General Data Protection Regulations (GDPR) and Data Protection Act 2018 to which it is subject 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 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 impose 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 GDPR and Data Protection Act

2018 and 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 Yorkshire Ambulance Service NHS Trust and the relevant Professional body (where applicable).

3.0 Policy Statements

3.1 Data Protection Principles

3.1.1 All processing of personal data and special categories of data undertaken by the Trust must comply with the following six principles:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

- The Trust will ensure that all personal data processing complies with at least one of the GDPR's Article 6 - **Lawfulness of processing** conditions (see section 3.2.1 for more information) and in the case of special categories of data additionally with one of the Article 9 – **Processing of special categories of personal data** conditions (see section 3.2.1 for more information). The most common Article 6 condition for the Trust's processing of patient information for health care purposes is that it is required for its public task (Art. 6(1)(e)) and in relation to the special categories of data the relevant condition will be that the processing is necessary for the provision of health and social care (Art. 9(2)(h)) Processing patient information under these conditions does not rely on the consent of the patient. The Trust will make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which personal data will be kept.

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;

- The Trust will maintain a Record of Processing Activity (ROPA) that will detail all of the purposes for which it processes personal data. If the reasons for processing this information are changed, the record will be updated and relevant data subjects will be informed.

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

- Personal data is collected for specific purposes. The Trust will ensure that the personal data it collects is not excessive in relation to those

purposes and that it is adequate and relevant enough to carry out the required function. If data is provided or obtained which is excessive for the purpose, it will be immediately deleted or destroyed.

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;**

- Where the Trust obtains information either directly from the data subject or via a third party, it will ensure the accuracy of the data. If the data subject informs the Trust of a (factual) inaccuracy, the data will be amended to reflect this, if this is agreed. Exceptionally a note will be appended to the record to indicate that the data subject does not agree that the data held is accurate.

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 GDPR in order to safeguard the rights and freedoms of individuals;**

- The Trust will not retain information for longer than it is required to fulfil the purposes for which it is collected. The Trust's retention schedule (within the Records Management Policy) and identified within the Record of Processing Activity will be used to ensure that it complies with this principle.

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.**

- All information relating to patients and staff must be kept secure at all times. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Trust and its processors has ensured there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Please refer to the Trust's ICT Security Policy and Associated Procedures, Email Policy, Internet Policy and Procedure and Records Management Policy for further information.

- All staff and personnel working for or on behalf of the Trust, including agency staff and contractors have an individual responsibility to maintain the security of personal information.

3.2 Legal bases for processing under the GDPR

3.2.1 The chart below describes the various legal bases for processing personal data under the GDPR that the Trust may rely upon for its various processing activities. It also includes links to the specific recitals and articles in the law that correlate to the bases.

Consent	Rec.32, 42, 43; Art.6(1)(a) Processing is permitted if the data subject has consented to the processing.
Contractual necessity	Rec.44; Art.6(1)(b) Processing is permitted if it is necessary for the entry into, or performance of, a contract with the data subject or in order to take steps at his or her request prior to the entry into a contract.
Compliance with legal obligations	Rec.45; Art.6(1)(c), 6(3) Processing is permitted if it is necessary for compliance with a legal obligation under EU law or the laws of a Member State.
Vital interests	Rec.46; Art.6(1)(d) Processing is permitted if it is necessary in order to protect the vital interests of the data subject or of another natural person.
Public interest	Rec.45; Art.6(1)(e) Processing is permitted if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
Legitimate interests	Rec.47, 48; Art.6(1)(f) Processing is permitted if it is necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests,

fundamental rights or freedoms of the affected data subjects which require protection, particularly where the data subject is a child. This does not apply to processing carried out by public authorities in the performance of their duties.

Additional powers for Member States

Rec.40; Art.6(2) Member States may introduce additional lawful bases in relation to processing carried out for the purposes of complying with legal obligations (see Art.6(1)(c) above) or performing tasks in the public interest (see Art.6(1)(e) above).

Data relating to criminal offences and civil law enforcement

Art.10, 23(1)(j) Personal data relating to criminal convictions and offences or related security measures may only be processed:

- under the control of an official authority; or
- when permitted under EU or member state law.

Any comprehensive register of criminal convictions may be kept only under the control of official authority.

Member States may impose restrictions on the processing of personal data for the purposes of enforcing civil law claims.

Processing Special Categories of Data

Rec.51-56; Art.9 The processing of Special Categories of Data is prohibited, unless:

- Art.9(2)(a) The data subject has given explicit consent.
- Art.9(2)(b) The processing is necessary in the context of employment law, or laws relating to social security and social protection.
- Art.9(2)(c) The processing is necessary to protect vital interests of the data subject (or another person) here the data subject is incapable of giving consent.
- Art.9(2)(d) The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes.
- Art.9(2)(e) The processing relates to personal data which have been manifestly made public by the data subject.
- Art.9(2)(f) The processing is necessary for the

establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.

- Art.9(2)(g) The processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects.
- Art.9(2)(h) The processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services.
- Art.9(2)(i) The processing is necessary for reasons of public interest in the area of public health(e.g., ensuring the safety of medicinal products).
- Art.9(2)(j) The processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.
- Art.9(4) Member states may maintain or introduce further conditions, including limitations with regard to genetic data, biometric data or health data.

Processing for new purposes

Where personal data are to be processed for a new purpose, the controller must consider whether the new purpose is "compatible" with the original purpose taking into account the following factors:

- any link between the original purpose and the new purpose;
- the context in which the data have been collected, including the controller's relationship with the data subjects;
- the nature of the personal data, in particular, whether Sensitive Personal Data are affected;
- the possible consequences of the new purpose of processing for data subjects; and
- the existence of appropriate safeguards (e.g., encryption or pseudonymisation).

3.3 Record of Processing Activity (ROPA)

3.3.1 As a data controller of personal data, the Trust needs to maintain a record of the following:

- The Trust’s name and contact details.
- The name and contact details of the Data Protection Officer – a person designated to assist with GDPR compliance under Article 37.

- The name and contact details of any joint controllers – any other organisations that decide jointly with the Trust why and how personal data is processed.
- The purposes of the processing – why the Trust uses personal data, e.g. direct health care, patient transport provision, recruitment.
- The categories of individuals – the different types of people whose personal data is processed, e.g. employees, patients, Trust members.
- The categories of personal data the Trust processes – the different types of information the Trust processes about people, e.g. health data, contact details, financial information.
- The categories of recipients of personal data – anyone the Trust shares personal data with, e.g. NHS organisations, suppliers, credit reference agencies, government departments.
- If applicable, the name of any third countries or international organisations that the Trust transfers personal data to – any country or organisation outside the EU.
- The safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the GDPR.
- The retention schedules for the different categories of personal data – how long you will keep the data for.
- A general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.

3.3.2 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 GDPR.

3.3.3 Failure to ensure that all processing of personal data is reflected within the Trust's ROPA constitutes an offence under the GDPR and Data Protection Act 2018 and may result in the Trust and/or individual staff facing prosecution.

3.4 Data Subject Rights

3.4.1 Data subjects (patients, staff and others) have the following rights regarding data processing and the personal data that are recorded about them by the Trust:

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; and

8. Rights in relation to automated decision making and profiling.

3.4.2 For processing to be lawful under the GDPR, the Trust must identify a lawful basis before it can process personal data. It is important that the Trust determines the lawful basis for processing personal data because this has an effect on the data subjects' rights. For instance, if the Trust rely on someone's consent to process their data, then they will generally have stronger rights to have their data deleted. Each of these rights are explained in further detail and how they impact on the Trust in the following sections.

3.4.3 The Trust will ensure that requests made by data subjects in relation to their rights regarding data processing are handled in accordance with the GDPR and Data Protection Act 2018 and Information Commissioners GDPR and Data Protection Act 2018 Legal Guidance. Process flow charts for handling data subject notices under the GDPR and Data Protection Act 2018, are detailed in Appendix G of this Policy.

3.5 Right to be Informed

3.5.1 The Trust will provide 'fair processing information', typically through a privacy notice published on the Trust's website, which provides transparency about how the Trust collect and use personal data. The information the Trust supplies in the privacy notice must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

3.5.2 If the Trust obtains the personal data directly from a data subject it must supply the privacy notice at the time that the data is collected.

3.5.3 If the Trust obtains the personal data from another source it must provide the data subject with the privacy notice within a reasonable period of having obtained the personal data (typically, within one month), or if the Trust is using the personal data to communicate with the data subject, at the latest, when the first communication takes place.

3.5.4 The Trust's privacy notices contain the following information:

- The identity and contact details of the data controller (and where applicable, the controller's representative) and the Data Protection Officer;
- The purpose and the lawful basis for the processing;
- The legitimate interests of the data controller or third party, where applicable;
- The categories of personal data being processed (only if the personal data is not obtained directly from the data subject);
- Any recipient or categories of recipients of the personal data;
- Details of transfers to a third country and the safeguards in place;
- The retention period or criteria used to determine the retention period of the personal data;
- The existence the data subject's rights;
- The right to withdraw consent at any time, if that is the lawful basis for the processing;
- The right to lodge a complaint with the Information Commissioner's Office (ICO);
- The source the personal data originates from and whether it came from publicly accessible sources (only if the personal data is not obtained directly from the data subject);
- Whether the provision of the personal data is a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data; and
- The existence of automated decision making, including profiling and information about how decisions are made, and the significance and the consequences of such automated decision making.

3.6 Right of Subject Access

3.6.1 Data subjects (patients, staff and others) are entitled to a copy of personal information held about them providing that the information falls within the remit of the GDPR and Data Protection Act 2018. All subject access requests must be directed to the Legal Services Department SubjectAccessRequests@yas.nhs.uk . On no account should a member of staff try to handle a request themselves.

3.6.2 The Trust must be able confirm that personal data is being processed and provide access to the personal data on request from a data subject. The GDPR allows data subjects to access their personal data so that they are aware of and can verify the lawfulness of the processing.

3.6.3 The Trust must be able to verify the identity of the person making the access request, using 'reasonable means' and it must provide a copy of the information free of charge. However, the Trust can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive (it can also refuse to respond to an access request under these circumstances). The Trust may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that it can charge for all subsequent access requests. Any fee charged must be based on the administrative cost of providing the information.

3.6.4 Any individual who wishes to exercise the right of subject access should apply in writing to the Legal Services Department. Any such request must be complied with promptly and in any event within one month of receipt of the written request and, where appropriate, the fee. This period may be extended by two further months where necessary, taking into account the complexity and number of requests. The Trust must inform the subject of any such extension within one month of receipt of the request, together with a reason for the delay.

3.6.5 For more information please refer to the Procedure for Handling Disclosure Requests under the GDPR and Data Protection Act (2018) within Appendix F of this Policy.

3.7 The Right to Rectification

3.7.1 Data subjects are entitled to have personal data rectified if it is inaccurate or incomplete. If the Trust has passed the personal data to third parties, it must inform the third parties of the rectification where possible. The Trust must also tell the data subjects about the third parties and what personal information it has passed to them.

3.7.2 The Trust must respond within one month to a data rectification request, but this can be extended by two months when the request for rectification is complex.

3.8 The Right to Erasure

3.8.1 Also known as 'the right to be forgotten', data subjects can request the deletion or removal of personal data where there is no compelling reason for its continued processing.

3.8.2 Data subjects do not have an absolute 'right to be forgotten' but the Trust must erase personal data and prevent processing in specific circumstances:

- When the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent and the Trust's lawful basis for processing relies on the data subject's consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed (in breach of some other aspect of the GDPR);
- The personal data has to be erased in order to comply with a legal obligation; or
- The personal data is processed in relation to the offer of information society services to a child.

3.8.3 The Trust can refuse to comply with a request for erasure when the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- The exercise or defence of legal claims.

3.9 Right to Restrict Processing

3.9.1 A data subject may require the Trust to stop processing their personal data when:

- the data subject contests the accuracy of the personal data;
- the Trust is processing the personal data for the performance of a public interest task or for the purpose of legitimate interests and it is considering whether the Trust's legitimate grounds override those of the data subject;
- processing is unlawful and the data subject does not require the personal data erased but requests restriction instead;
- the Trust no longer need the personal data but the data subject requires the personal data to establish, exercise or defend a legal claim.

3.9.2 When processing is restricted, the Trust is permitted to store the personal data, but it must not process it. The Trust can retain just enough information about the data subject to ensure that the data processing restriction is respected in future.

3.9.3 If the Trust has disclosed the personal data in question to third parties, it must

inform them about the restriction on the processing of the personal data, unless it is impossible to do so.

3.10 Right to Data Portability

3.10.1 The right to data portability only applies:

- to personal data which a data subject has provided to the Trust;
- where the processing is based on the data subject's consent or for the performance of a contract;
- when processing is carried out by automated means.

3.10.2 If any of these conditions apply then the Trust must provide the personal data in a structured, commonly used and machine readable form such as CSV or XML files. This enables other organisations to easily use the data. The Trust may be required to transmit the data directly to another organisation if this is technically feasible.

3.10.3 The Trust must respond within one month and it may not charge for providing the personal data. If it is unable to supply the personal data because the request is complex or the Trust receives many requests from the data subject then it must inform the data subject of this within one month and can extend the time to comply with the request by a further two months.

3.11 Right to Object

3.11.1 Data subjects must be informed of their right to object "at the point of first communication" and in the Trust's privacy notice. This information must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information" and it must offer an online way for data subjects to object to the processing of their personal data.

3.11.2 If the Trust processes personal data for the performance of a legal task or under its legitimate interests then data subjects can object to the processing of their personal data only on "grounds relating to his or her particular situation". Once the Trust receives an objection it must stop processing the personal data unless it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual or the processing is for the establishment, exercise or defence of legal claims.

3.11.3 If the Trust processes personal data for direct marketing purposes then it must stop processing personal data for direct marketing purposes as soon as it receives an objection and it cannot refuse to do this. Objections about direct marketing must be dealt with at any time and the Trust may not charge for this.

3.11.4 If the Trust processes personal data for research purposes then data subjects

can object to the processing of their personal data only on “grounds relating to his or her particular situation”. The Trust does not need to take note of an objection if it is conducting research which is necessary for the performance of its public task.

3.12 Rights in Relation to Automated Decision Making and Profiling

3.12.1 The Trust should continually monitor and identify whether any of its processing operations constitute automated decision making or profiling and consider whether it needs to update the Trust’s procedures to deal with the requirements of the GDPR.

3.12.2 Decisions about data subjects must not be taken by automated means if the decision would produce a legal effect or similar significant effect. However, the Trust can use automated decision making if the decision is necessary for entering into or for the performance of a contract with the data subject; if the decision is authorised by law, or if the data subject provides explicit consent. If the Trust does use automated decision making in these cases then it must provide data subjects with access to human intervention, with the ability to provide their point of view and with an explanation of the decision and how it can be challenged.

3.12.3 Profiling is any form of automated processing which evaluates certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location;
- movements.

3.12.4 If the Trust uses automated profiling it must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the likely consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement technical and organisational measures to enable inaccuracies to be corrected and to minimise the risk of errors.
- Secure personal data so that the interests and rights of data subjects are not compromised.

3.12.5 The Trust must not automate decisions about children, or automate decisions about any data subjects based on the processing of the special categories of data unless it has explicit consent from the data subject or if the processing is being carried out for reasons of substantial public interest.

3.13 Application of the Data Subject Rights

3.13.1 The availability of rights for data subjects largely depends on the Trust's legal basis for processing. The table below summarises when rights are available.

Legal Basis	Right to:				
	Object	Erasure	Automated decision making	Rectification	Portability
Consent	X (but can withdraw consent)	✓	X (but can withdraw consent)	✓	✓
Contract	X	✓	X	✓	✓
Legal Obligation	X	X	X	✓	X
Vital Interest	X	✓	X	✓	X
Public task	✓	X	✓	✓	X
Legitimate Interests	✓	✓	✓	✓	X

3.14 Refusal of Data Subject Rights

3.14.1 If the Trust decides not to carry out a request for data access, rectification or data portability, it must provide an explanation to the data subject and inform them of their right to complain to the ICO and to a judicial remedy.

3.15 Data Protection Complaints and/or Enquiries

3.15.1 Complaints about the Trust's Data Protection procedures and appeals against decisions not to supply exempt information will be dealt with by the Data Protection Officer, who will deal with the complaint in accordance with the Trust's Complaints Policy.

3.15.2 General enquiries about the GDPR or Data Protection Act will be dealt with through the Information Governance Manager who will provide advice to the relevant department of the Trust in support of the resolution of the enquiry.

3.16 Consent and Fair Processing

3.16.1 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.

3.16.2 Under 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.

3.16.3 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.

3.16.4 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 controller and 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 GDPR, which would normally be 'official authority vested in the controller' or 'contract', in these cases the official authority or relevant part of the contract will be identified.

3.16.5 Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR clarifies that silence, pre-ticked boxes or inactivity does not constitute consent.

3.16.6 Where patients have been informed of:

a) the use and disclosure of their information associated with their healthcare; and
b) 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.

3.16.7 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.

3.16.8 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.

3.16.9 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, not just financial matters, once they lose the ability to do so. The Mental Capacity Act (2005) 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.

3.16.10 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.

3.16.11 The Trust will 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. Whichever is the appropriate condition for a particle processing activity this will be clearly identified in the Trust's ROPA. Forms (whether paper-based or web-based) that gather personal data relating to a staff member must contain a statement explaining what the information is to be used for and to whom it may be disclosed.

3.16.12 All staff should be aware that the Trust publishes a number of items that include personal data and will continue to do so. These personal data are:

- Names of all members of Trust committees (including the Board, charities, Committee and Audit Committee)
- Names, job titles and academic and/or professional qualifications of members of staff
- Awards and honours
- Staff qualifications, long service awards, etc
- Videos or other multimedia versions of training exercises and ceremonies
- Information in staff magazines (including photographs), annual reports, staff newsletters, etc
- Staff information on the Trust intranet (including photographs)

3.16.13 It is recognised that there might be occasions when a member of staff requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals will be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Trust will comply with the request and ensure that appropriate action is taken.

3.16.14 It is particularly important to obtain consent if a staff members data is to be published on the internet as such data is then in the public domain.

3.17 Disclosure of personal data and special categories of data without Consent

3.17.1 A number of Acts of Parliament govern the disclosure/sharing of personal data and special categories of data. Some make it a legal requirement to disclose whilst others state when information cannot be disclosed. The Confidentiality: NHS Code of Practice (2003) gives clear guidance on disclosure of patient identifiable information.

3.17.2 Legislation to restrict disclosure:

- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976

3.17.3 Legislation requiring disclosure:

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunizations and vaccinations to NHS Trusts from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

3.17.4 There are only three exceptional circumstances that disclosure without consent in a patient with capacity may be justified. These are where:

- Statute law requires,
- There is a court order,
- Disclosure may be necessary in the public interest where a failure to disclose information may expose others to risk of death or serious harm.

3.17.5 The courts, including coroner's courts, some Tribunals and persons appointed to hold inquiries have legal powers to require disclosure of information that may be relevant to matters within their jurisdiction. This does not require the consent of the patient, whose records are to be disclosed. Such disclosures must be strictly in accordance with the terms of a court order and should only provide the required information to the bodies specified in the order.

3.17.6 Disclosures in the public interest may be necessary to prevent serious crime or risk of significant harm. Public interest is described as exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.

3.17.7 Serious crime can be defined as cases involving murder, manslaughter, rape, treason, kidnapping and child abuse and may all warrant disclosure of confidential information in the public interest. Significant harm to the security of the State or public order also fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally

not warrant breach of confidence.

3.17.8 The Trust will observe and adhere to all legislation relating to the disclosure of personal data and special categories of data. Any disclosure of information should be proportionate and limited to relevant details following the Caldicott Principles. Each case must be considered on its own merits.

3.17.9 The Trust's Legal Services Department oversee all disclosures of patient identifiable data and subject access requests for staff identifiable data, health

3.18 Information Sharing Protocols

3.18.1 The Trust is currently a signatory to a number of regional information sharing protocols which provide the basis for facilitating the lawful exchange of personal data and special categories of data between health and partner organisations. Information sharing protocols and agreements do not in themselves make the exchange of personal data and special categories of data lawful.

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

3.18.3 The Trust will ensure it adheres to the various regional protocols and is proactive in putting specific information sharing agreements in place when required.

3.19 Research

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

3.19.2 Personal data processed for research purposes only, receives certain exemptions from the 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.

3.19.3 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.

3.19.4 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.

3.19.5 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.

3.20 Anonymisation and Managing Data Protection Risk

3.20.1 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 Governments 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.

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

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

3.21.1 The Trust will ensure that procedures and guidance are in place to enable compliance with Principle F – Providing appropriate security, of the GDPR and Data Protection Act 2018. This principle requires that "*appropriate organisational and technical measures*" must be taken in the protection of personal data and special categories of data.

3.21.2 All staff must adhere to basic principles for preventing theft, fraud and confidentiality and security breaches e.g. shutting and locking the door to a secure area and not leaving ID cards lying about. 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

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

- Comply with the 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 full

anonymised and does not breach the GDPR and Data Protection Act 2018 (refer to the Management of Online and Digital Services Procedure for mandated requirements).

- Ensure when anonymised or pseudonymised information is shared, care is taken to ensure that the method used to anonymised 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 to hold and process it securely 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 e.g. CD, DVD 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 Trusts 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.
- Ensure staff 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 and adhere to safe haven principles (see Appendix D).
- 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 information 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.

3.21.4 In order to comply with legislation and Department of Health guidance, the Trust adheres to Safe Haven principles to safeguard the confidentiality of patient and staff information held and transferred. The term 'Safe Haven' is used to describe either:-
(1) a secure physical location, or (2) the agreed set of administration arrangements that are in place within the Trust to ensure confidential patient or staff information is communicated safely and securely.

3.21.5 Safe haven principles and procedures must be in place in any location where personal information is being received, held or communicated especially where the personal information is of a confidential and sensitive nature. Safe

havens principles enable staff to be confident that information can be transferred securely between environments.

3.21.6 All members of staff handling confidential patient and staff information, whether paper based or digital (computerised) must adhere to the safe haven principles. Please see Appendix D Safe Haven Principles: Guidance on the Secure Transfer of Confidential Information.

3.21.7 The Trust does not support the use of fax machines for the routine transfer of person data and special categories of data and its use should be avoided wherever possible. Where it is necessary and there is no secure alternative to transfer personal data on an ad hoc basis by fax, safe haven principles and procedures must be followed. Please see Appendix D. Information Asset Owners are expected to take proactive steps to implement secure alternatives for the transfer of personal data and special categories of data.

3.21.8 All staff must adhere to the following related policies:

- ICT Security Policy and Associated Procedures
- Email Policy
- Internet Policy and Procedure
- Records Management Policy
- Management of Online and Digital Services Procedure
- Social Media Policy
- Safety and Security Policy

3.22 Data Protection Impact Assessments

3.22.1 Data Protection Impact Assessments (DPIAs), also known as Privacy Impact Assessments (PIAs) are a tool recommended by the Information Commissioner's Office to build Data Protection Act 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.

3.22.2 Under the GDPR and the Data Protection Act the Trust must undertake a DPIA for certain types of processing, or any other processing that is likely to result in a high risk to individuals.

3.22.3 The Trust must do a DPIA before it begins any type of processing which is "likely to result in a high risk to individuals". This means that although the actual level of risk may not have yet been assessed the factors that point to the potential for a widespread or serious impact on individuals must be considered. In particular, Information Asset Owners and/or project managers must ensure that a DPIA is undertaken in all instances where a new project or initiative will:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

3.22.4 A DPIA should also be completed if there is a plan to:

- use new technologies;

- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

3.22.5 The Data Protection Officer (DPO) should be consulted on all DPIAs and, where appropriate, individuals and relevant experts. Any data processors may also need to be involved in the assessment.

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

3.22.7 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

3.22.8 It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

3.22.9 A DPIA may not be required if:

- The processing is on the basis of legal obligation or public task. However, this exception only applies if:
  - there is a clear statutory basis for the processing;
  - the legal provision or a statutory code specifically provides for and regulates the processing operation in question;
  - a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted. This may not always be clear, and in the absence of any clear and authoritative statement on whether such an assessment was conducted it is recommend that you err on the side of caution and conduct a DPIA to ensure you consider how best to mitigate any high risk.

3.22.10 The Trust's Data Protection Impact Assessment Procedure can be found in Appendix E.

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 GDPR or Data Protection Act undertakings, enforcement notices, 'stop now' orders, compulsory assessment notices or monetary penalty notices are served on the organisation by the Information Commissioners Office.

6.2 Information Governance incidents will be monitored by both the Clinical Governance Group and the Information Governance Working Group.

6.3 The Quality Committee will monitor overall progress through receipt of quarterly reports in relation to full compliance against the 10 Data Security Standards of the Trust's Data Security and Protection Toolkit . The Information Governance Working Group 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 References

- Great Britain. 2018. Data Protection Act 2018. London: HMSO. Available at: www.legislation.gov.uk
- European Union. 2016. EU General Data Protection Regulations 2016. Available at: www.eugdpr.org
- Great Britain. 2000. Freedom of Information Act 2000. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2004. Environmental Information Regulations 2004. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. Computer Misuse Act 1990. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. Access to Health Records Act 1990. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1958 and 1967. Public Records Act 1958 and 1967. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. Crime and Disorder Act 1998. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. Electronic Communications Act 2000. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. Human Rights Act *1998*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. The Regulation of investigatory Powers Act 2000. London: HMSO. Available at: www.legislation.gov.uk
- Information Commissioner's Office (ICO). Publications: GDPR and Data Protection Act 2018 Legal Guidance. Available at: www.ico.gov.uk
- Department of Health, 2000. Publications: Information Governance Toolkit. Available at: https://nww.igt.hscic.gov.uk/
- Information Commissioner's Office (ICO). Publications: Anonymisation: Managing Data Protection Risk Code of Practice, 2012. Available at: www.ico.gov.uk
- Information Standards Board Publication: Anonymisation Standard for Publishing Health and Social Care Data, 2013. Available at: http://www.isb.nhs.uk
- Department of Health, 2013. Publications: Information: To Share or Not to Share? The Information Governance Review. Available at: https://www.gov.uk
- The Health and Social Care Information Centre 2013. Publications: A Guide to Confidentiality in Health and Social Care. Available at: http://www.hscic.gov.uk

8.0 Appendices

Appendix A The Caldicott Principles

All staff must apply the general principles of good practice in handling and use of patient identifiable information:

- **Justify the purpose(s)**
  Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian
- **Don't use patient identifiable information unless it is absolutely necessary**
  Patient-identifiable information items should not be used unless there is no alternative
- **Use the minimum necessary patient identifiable information**
  Where use of patient identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification
- **Access to patient-identifiable information should be on a strict need to know basis** Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see
- **Everyone should be aware of their responsibilities**
  Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are aware of their responsibilities and obligations to respect patient confidentiality
- **Understand and comply with the law**
  Every use of patient identifiable information must be lawful. The Trusts Caldicott Guardian is responsible for ensuring that the organisation complies with the Caldicott Principles
- **The duty to share information can be as important as the duty to protect patient confidentiality**
  Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix B Definitions

The definitions or explanation of terms relating to this policy are:-

Personal Data	Personal Data is any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.
Special Categories of Data	Special Categories of Data is any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Data Controller	The entity that, alone or jointly with others, determines the purposes, conditions and means of the processing of personal data.
Data Processor	An entity that processes data on behalf of the Data Controller.
Data Subject	Any natural person whose personal data is processed by a controller or processor.
Processing	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosureby 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. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Consent does not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority, such as an Ambulance Trust, is processing the data in the performance of its public task, and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.

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.
Disclosure	This is the divulging or provision of access to data.
Bulk Transfer	The transfer of electronic or paper data that is ‘batched up’ to be sent out of a location and/or organisation.
Approved Courier	A courier on an authorised list of trusted and reliable courier services for routine and secure courier transfers, as agreed by the Trust.
Anonymised	Irreversible removal of identifying data.
Pseudonymised	It differs from anonymisation, which is characterised by the irreversible removal of identifying data. Pseudonymised data continues to be "personal data" for the purposes of the GDPR and Data Protection Act 2018. Pseudonymisation is a process which involves the removal of identifying information from data but does so in such a way as to allow the data to be restored to an identifiable format when required.

Appendix C Roles & Responsibilities

Chief Executive
The Chief Executive has overall responsibility for compliance with the 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 SIRO under delegated authority from the Chief Executive, oversees compliance with the Data Protection Act and the development of appropriate policy and procedure. The SIRO is supported by the Data Protection Officer, Information Asset Owners, Legal Services Manager and Information Governance Manager. The SIRO is responsible for ensuring any suspected or actual breach of the Act is investigated and appropriate action taken.

Data Protection Officer
The nominated Data Protection Officer is responsible for monitoring internal compliance, informing and advising the Trust on its data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the Information Commissioners Office, and for advising on day-to-day data protection matters.

Legal Services Manager
The Legal Services Manager is responsible for ensuring strict compliance with the Data Protection Act in relation to disclosure of health records and person identifiable information.

Information Governance Manager
The Information Governance Manager is responsible for providing general guidance and advice on data protection and the application of this policy.

Information Asset Owners and Line Managers
Information Asset Owners and all line managers have responsibility for ensuring that their staff are compliant with, and working to, all relevant policy and procedure in relation to Data Protection as well as championing good information handling practices within the Trust.

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 Yorkshire Ambulance Service.

Any incident involving a breach or suspected breach of the GDPR or Data Protection Act must be reported immediately via the Datix incident reporting system.

Appendix D

Yorkshire Ambulance Service NHS
NHS Trust
An Aspirant Foundation Trust

Safe Haven Principles: Guidance on the Secure Transfer of Confidential Information

This guidance applies to all records in whatever media they may be held (e.g. paper, electronic files and emails, images and audio recordings), which include personal data or special categories of data relating to patients, staff or others.

Safe Haven Principles: Internal and External Post

- Ensure envelopes containing confidential information are sealed and marked 'private and confidential'.
- Double check the full postal address (including postcode) of the recipient is correct.
- Ensure internal mail has been addressed fully and correctly, providing at least the following basic information;
  - First Name and Surname - *Mrs Annette Curtain*
  - Department - *Finance Department*
  - Site – *Spring Hill 1*
- If addresses are handwritten please make them legible for the post room staff.
- Cross out the previous address on internal envelopes to stop any confusion on the next recipient.
- Use two envelopes for bulky letters for extra security.
- Take care when using window envelopes that the correct, full address is visible. No other information should be visible.
- Use only the correct, sealed record bags and wallets for transferring patient care records via the Trusts internal transport service to Healthcare Records. Patient care records must not be placed in the internal or external post to transfer them to Healthcare Records.
- Make sure that inbound post is handled promptly and securely around the workplace.
- Ensure you have a designated area within your Department or Station for mail collection and deposit. In the absence of defined lockable and managed post rooms at most Trust sites, any inbound or outbound mail (this includes staff payslips) which is to be left uncollected and unattended on Station or at any YAS site, for any length of time, should be locked away in a specially designated locked drawer or locked filing cabinet or within an office which is kept locked when not in use, ideally within the station managers office. Existing pigeon hole systems can be used if they are within an internal locked office
  .
- Routine transfers of personal data or special categories of data by internal or external post must be recorded on your departmental data flow records.

Safe Haven Principles: Royal Mail Special Delivery and Courier Services (full tracked services)

- Seek advice from your line manager or the Information Governance Manager on whether Royal Mail Special Delivery or other approved courier service should be used for ad hoc transfers of confidential information externally.
- Due to the added cost of sending items of post by Royal Mail Special Delivery or approved courier service, a risk assessment should be undertaken which

considers the sensitivity of the information and number of identifiable individuals whose information is recorded.

- Computer media containing confidential information must not be transferred unless it is an encrypted copy of the original. It should only be transferred by Royal Mail Special Delivery or approved courier service. There are also additional requirements around removable media and bulk transfers (see below).
- Let the recipient know when to expect receipt of the item and ask the recipient to confirm receipt. The above principles relating to internal and external post also apply when using Royal Mail Special Delivery or approved courier services.
- Routine transfers of personal data or special categories of data by Royal Mail Special Delivery or approved courier must be recorded on your departmental data flow records.

Safe Haven Principles: Bulk Transfers

- Bulk transfers of personal data or special categories of data must have the approval of the relevant Information Asset Owner (IAO).
- When transferring bulk personal information you must use an approved courier or secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.
- When transferring personal information by approved courier:
    a) The individual responsible for passing the information to the courier must check the ID of the courier and obtain a receipt from the courier when the bulk personal information is collected.
    b) The sender must confirm the bulk transfer has been received by contacting the recipient.
    c) The courier must only hand this information over to the recipient or to a nominated individual and obtain a signature when delivered.

Safe Haven Principles: Removable Media

- The use of removable media such as CDs and DVDs for the writing of personal data or special categories of data, is prohibited other than for the approved transfer of large volumes of data where an alternative secure means of transfer (e.g. secure file transfer protocol or NHS Mail) is not feasible.
- Electronic personal information to be sent via removable media by post or courier must be encrypted to 256 bit AES encryption prior to transfer, in line with Department of Health encryption requirements. The transfer must be approved by the Trust's Senior Information Risk Owner (SIRO).
- Information held on the removable media device must be securely erased or disposed of once the transfer is complete.

Safe Haven Principles: Pigeon-holes/In trays for paper information

- Regular housekeeping must be carried out in areas where pigeon holes or in-trays are used to disseminate corporate and person identifiable information.
- Nothing should be left in these areas overnight especially in relation to sensitive information unless the area is secured.

Safe Haven Principles: Use of the Telephone

- Personal information must only be given over the telephone if you are confident of the identity of the caller. If you are not, you must always take a number, verify it independently and call back. When speaking to a patient or carer on the telephone, confirm the caller's identity or ring back.
- Always check whether an individual is entitled to the information they request. Information relating to patients must only be released on a need-to-know basis and with

consent in most instances. Legal Services Department handle all disclosures of patient identifiable information.

- If you receive suspicious queries asking the whereabouts, base or personal information of other staff members, please treat with caution, take contact details of the caller and verify that it is an authorised person and request.
- Report any suspected bogus enquires to your line manager and as an incident on the Datix system.
- Messages about named patients must not be left on answerphones. Simply leave your name and telephone number and no other information.
- Ensure unauthorised people cannot overhear you when making sensitive telephone calls, during meetings, and when you are having informal discussions with colleagues about personal/business sensitive information. In these situations, if you do not need to identify a patient or staff member by name, then don't.

Safe Haven Principles: Transcribing of telephone messages

- Recorded telephone messages containing person identifiable information including sensitive information such as the names and addresses of applicants telephoning for a job application, or patient details must be received in to a secure location, so that only those entitled to listen to the message may do so whilst it is being played back.
- If you use any kind of message book e.g. to note messages for absent staff members, this should also be stored securely.

Safe Haven Principles: Fax Transmission

- Fax is inherently insecure and is not recommended for transfer of personal information.
- Fax machines should only be used to transfer patient or staff-identifiable information where it is absolutely necessary to do so and there is no secure alternative.
- Always use a fax cover sheet to enforce the confidentiality of the message.
- Telephone the recipient of the fax (or their representative) to let them know you are sending them confidential information. Ask them to wait by the fax machine whilst you send your message through to them.
- Send a test fax transmission when sending to a new fax number.
- Send information to a Safe Haven fax whenever possible.
- Always double check the fax number before you hit the send button, whether the fax is Safe Haven or not.
- Use pre-installed numbers wherever possible to minimise the risk of dialling a wrong number.
- Request a report sheet that confirms your transmission has been successful.
- Ask the recipient to let you know when they receive the fax.
- Anonymise patient details wherever possible, but don't compromise patient safety.

Safe Haven Principles: Taking Paper Based Confidential Documents Off Site

- When working off-site the use of paper-based records containing patient or staff-identifiable information should be kept to a minimum. This also extends to any other information which the Trust deems to be of a confidential and sensitive nature eg commercially sensitive information such as a tender document.
- There must be a clear requirement to take such information off-site in the first instance and when doing so, responsibility lies solely with you.
- Staff who have a clear business need to use paper-based copies of documents containing personal information off-site must adhere to the following:

- Where the transfer is not an approved and acknowledged routine transfer for business purposes, make sure that your immediate line manager is aware that you have a requirement to take confidential information off-site and gain approval.
- Keep equipment and paper-based records/files locked and out of sight during transit.
- Keep usage to a minimum in public areas.
- Ensure the security of information ie store it in a locked container (eg a filing cabinet, lockable briefcase). If this is not possible, when not in use, information should be neatly filed and stored away.
- Do not dispose of any documents unless they can be shredded.
- Ensure that the information is returned to Trust premises as soon as possible and filed accordingly.
- Consider scanning the documents and then accessing them from a secure area via a Trust laptop.

Safe Haven Principles: Mobile Computing

- All devices must be operated in a secure manner at all times.
- When not in use, devices should be kept in a secure place.
- Do not leave any device visible in an unattended vehicle.
- The amount of information that is kept on the device should be kept to a minimum.
- All information should be stored on the Trust's servers where it is regularly backed-up.
- Details of any password or PIN must be kept secure.

Safe Haven Principles: Trust Laptops and Tablet Devices

- Laptops and tablets left on display and unattended will inevitably attract attention and have the potential to be stolen. The security of your work laptop or tablet device is your responsibility. Please ensure that you adhere to the following:
- Ensure that your device is placed in a secure, locked location (eg desk drawer, filing cabinet) when not in use or left overnight on work premises.
- Ensure that your device is not left unattended in an insecure area where members of the public may have access (eg meeting rooms or hotel rooms). Always use lockable storage facilities where available.
- Be aware of opportunist or targeted thefts of laptop bags in busy public places, such as airports, train stations, hotel receptions and exhibition halls and on public transport.
- Ensure your device is stored securely and out-of-sight when travelling and not in use. When travelling by car, ensure your device is locked in the boot and never left on car seats or foot wells. Devices should be removed from cars if they are going to be left unattended for any length of time.
- Avoid leaving devices in locations where they could be easily forgotten or left behind eg overhead racks on trains or in the boot of a taxi.
- Specifically when working from home on your device:
- Ensure reasonable steps are taken to minimise visibility of your device from outside your home.
- Secure windows and doors when the home is unoccupied. Ensure blinds or curtains are closed.
- Make use of room locks and lockable storage facilities to secure your device.

- Where the option is available, always lock the device by pressing Control, Alt and Delete at the same time on your keypad and selecting the 'lock computer' option (alternatively press the Windows and 'L' keys together). This applies no matter how long you are leaving your device unattended for.
- Ensure that no other person eg family member of friends are allowed to access your device.
- Ensure that your device is connected to the Trust's network at least once a month, to enable the automated update of antivirus software and other security features.
- On no account should you store any patient or staff-identifiable information on personal computer devices.

Safe Haven Principles: USB Devices

- If you require a memory stick (USB device) you must apply for an encrypted USB device that is approved by the Trust. Please contact the ICT Service Desk via the self-service portal on the YAS intranet http://swkservicedesk.yas.nhs.uk/Portal/ and they will provide you with an application form. On collection, you will be given an instruction sheet and a password to unlock the device.
- If you have a requirement to take your USB device off-site, please ensure that you adhere to the following:
- Whilst in transit, carry the device discretely in a closed container or bag and not on public view where it can attract attention.
- Store the device in a safe and secure environment when working off-site.
- Where practical, mark the device to identify its ownership by the Trust.
- Be sure that an encrypted USB device is the most appropriate solution for storing work files. Make use of the secure drives and folders which enable you to share work across the Trust's computer network.

Safe Haven Principles: Email

- Please refer to the Trust's Email Policy for the mandatory and best practice requirements for the transfer of personal data, special categories of data and commercially sensitive information by email.
- Emails containing personal data, special categories of data and commercially sensitive information must only be transmitted to recipients outside of the Trust's secure email network by using one of the three methods detailed below:-
  1. By use of NHS Mail (both the sender and the recipient of the email MUST be using NHS mail email addresses or email addresses that are part of the Government Secure Intranet). NHS Mail is also widely known as NHS.net email.
  2. By encryption (to 256 bit AES) of the information within a strongly password protected file attached to the email correspondence. The Trust supports the use of WinZip for file encryption. Staff should contact the ICT Service Desk in relation to access to WinZip.
  3. By Secure File Transfer Protocol (SFTP)
- Strong passwords must be eight characters, alpha numeric, mixed upper and lower case.
- All transfers of person identifiable information, sensitive person identifiable information and commercially sensitive information outside of the Trust's secure email network must be authorised by a Departmental Information Asset Owner or Head of Department.

Appendix E

Yorkshire Ambulance Service NHS Trust

An Aspirant Foundation Trust

Data Protection Impact Assessment Procedure

Document Reference	PO – Data Protection Impact Assessment Procedure – May 2018
Version	V2.1
Responsible Committee	Trust Management Group
Responsible Director (title)	Steve Page, Executive Director of Quality, Governance and Performance Assurance/ Deputy Chief Executive
Document Author (title)	Allan Darby, Information Governance Manager
Approved By	Trust Management Group
Date Approved	
Review Date	
Equality Impact Assessed (EIA)	Yes
Protective Marking	Not protectively marked

t

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
1.0	February 2012	David Johnson	A	Initial version produced.
1.1	August 2013	Caroline Squires	A	Incorporation into Data Protection Policy and the agreed policy and procedural document format.
1.2	Oct 2015	Caroline Squires	D	Minor updates for accuracy
2.0	Nov 2015	Caroline Squires	A	Approved by TMG
2.1	Apr 2018	Allan Darby	D	Fully amended to reflect the requirements of the GDPR and the DPA 2018

A = Approved D = Draft

Document Author = Caroline Squires, Information Governance Manager

Associated Documentation:

Data Protection Policy and Associated Procedures
Data Protection Policy - Local Care Direct
Information Governance Policy
Information Governance Strategy
Management of Online and Digital Services Procedure
Internet Policy and Procedure
Email Policy
ICT Security Policy and Associated Procedures
Records Management Policy
Safety and Security Policy
Social Media Policy

1.0 Introduction

1.1 Data Protection Impact Assessments (DPIAs), also known as Privacy Impact Assessments (PIAs), are a tool recommended by the Information Commissioner's Office to build Data Protection Act 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.

1.2 A Data Protection Impact Assessment (DPIA) is a key component of a 'Privacy by design' approach to a project or other personal data processing activity (hereafter referred to as an 'initiative'). 'Privacy by design' is an essential tool in minimising privacy risks and building trust. The Information Commissioner's Office (ICO) encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any initiative, and then throughout its lifecycle.

1.3 This procedure explains how to carry out a Data Protection Impact Assessment (DPIA). It builds on the more general guidance issued by the Information Commissioner's Office.

What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a structured approach to identifying the privacy risks associated with the processing of personal data and for implementing appropriate controls to manage those risks. The process comprises the following six distinct steps and a parallel stream of consultation:

1. Identify the need for a DPIA
2. Describe the information flows
3. Identify and assess the privacy risks
4. Identify and approve controls
5. Assign responsibility for implementing controls
6. Re-assess and accept the risks.

Why conduct a DPIA?

Key benefits of conducting a DPIA are:

- Fulfilling the Trust's legislative, statutory and contractual obligations, particularly those under data protection legislation in relation to data processing activities
- Contributing towards effective risk management and increased privacy and data protection awareness across the Trust
- Giving individuals confidence that the Trust is taking steps to safeguard their privacy, and a better understanding of the ways in which their personal data are being used
- Taking actions which are less likely to be privacy intrusive and have a negative impact on individuals
- Increasing the likelihood that the initiative is more successful because privacy risks are identified early, allowing controls to be designed in at less cost and with less impact on delivery.

Is a DPIA required?

A DPIA is mandatory for any type of processing which is “likely to result in a high risk to individuals” but should also be completed for any initiative that involves the processing of personal data or any other activity that could impact the privacy of individuals. Examples are:

- Building a new IT system for storing or accessing staff personal data
- Implementing surveillance technology in a building, such as a CCTV system
- Using a cloud service for the storage of research data
- Developing policies or strategies that have privacy implications.

A DPIA should be completed for new initiatives or for changes to existing systems or processes. It may also be a recommended outcome from a formal investigation into an information security incident or weakness at the Trust.

The first step in conducting a DPIA is a screening process to decide whether the detailed work in the subsequent steps will be required.

A DPIA must be completed for all research projects that may impact the privacy of indviduals and/or involve the use of personal data.

When should a DPIA be undertaken?

Ideally, a DPIA should be undertaken in the early stages of an initiative. The earlier a DPIA is completed, the easier it is likely to be to address any privacy risks identified.

Who should conduct a DPIA?

The Trust’s Data Protection Officer has overall accountability for ensuring that DPIAs are completed for high risk personal data processing initiatives.

Responsibility for ensuring that a specific DPIA is completed lies with the individual responsible for the initiative, such as:

- The Information Asset Owner
- The project sponsor/manager
- The lead for a research project.

Who should hold the completed DPIA?

The individual responsible for the initiative should retain the master copy of the completed DPIA for audit purposes and to be able to demonstrate compliance with legislative requirements should a query be raised and a copy forwarded to the Information Governance Manager who will maintain a central register. The Trust's Data Protection Officer may request copies of DPIAs for monitoring and reporting purposes.

The Trust's DPIA template

The IAO or Project Manager should complete the Trust's standard Data Protection Impact Assessment Template at Appendix A of this procedure.

2.0 Purpose/Scope

2.1 Under the GDPR and the Data Protection Act the Trust must undertake a DPIA for certain types of processing, or any other processing that is likely to result in a high risk to individuals.

2.2 The Trust must do a DPIA before it begins any type of processing which is “likely to

result in a high risk to individuals". This means that although the actual level of risk may not have yet been assessed the factors that point to the potential for a widespread or serious impact on individuals must be considered. In particular, Information Asset Owners and/or project managers must ensure that a DPIA is undertaken in all instances where a new project or initiative will:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

2.3 A DPIA should also be completed if there is a plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

2.4 The Data Protection Officer (DPO) should be consulted on all DPIAs and, where appropriate, individuals and relevant experts should also be engaged. Any data processors may also need to be involved in the assessment.

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

2.6 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

2.7 It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

2.8 A DPIA may not be required if:

- The processing is on the basis of legal obligation or public task. However, this exception only applies if:
    - there is a clear statutory basis for the processing;
    - the legal provision or a statutory code specifically provides for and regulates the processing operation in question;
    - a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted. This may not always be clear, and in the absence of any clear and authoritative statement on whether such an assessment was conducted it is recommend that you err on the side of caution and conduct a DPIA to ensure you consider how best to mitigate any high risk.

3.0 Process

3.1 Step One - Identify the need for a DPIA

Complete the DPIA screening questions in the DPIA template. If the answer to any of the screening questions is 'Yes', a DPIA is required. Below are the screening questions, with some additional context and examples to help determine answers.

	Question	Context	Example
1	Does the initiative involve evaluating or scoring individuals (including profiling and predicting)?	This is particularly important when personal data processing relates to an individual's performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.	Building behavioural or marketing profiles of individuals based on their web activity.
2	Does the initiative involve automated decision-making that may have a significant effect on an individual?	This is personal data processing that aims to make automated decisions about individuals that produce legal effects or similarly significant effects upon the individual.	Asking an individual to submit personal data that is then analysed by a computer system, with the result that the individual's request to use a service is either accepted or refused.
3	Does the initiative involve systematic monitoring?	This is personal data processing used to observe, monitor or control individuals.	Installing a CCTV system on Trust premises.
4	Does the initiative involve the processing of 'special categories of data'?	Special categories of data is a particular set of personal data, as defined by data protection legislation (see the Definitions at Appendix B of the Data Protection Policy and Procedure).	Processing the health data of research participants in a research project.
5	Does the initiative involve processing personal data on a large scale?	There is no specific definition of 'large scale' but the following should be considered: • The number of individuals affected	Implementing a new patient record system.

		• The volume of personal data • The range of personal data • The duration or permanence of the processing activity • The geographical extent of the processing activity.	
6	Does the initiative involve datasets that have been matched or combined?	This relates to combining personal data originating from two or more personal data processing operations performed for different purposes or by different data controllers in a way that would exceed the reasonable expectations of the individual.	Matching patient or staff personal data against personal data held by a third party for profiling purposes.
7	Does the initiative involve the personal data of vulnerable people?	This relates to the processing of personal data where there is an imbalance of power between the individual and the Trust, or the processing involves a vulnerable section of society.	Processing children's personal data as part of a 'widening participation' activity in the Trust.
8	Does the initiative involve the use or application of innovative technological or organisational solutions?	New technology can often involve novel ways of collecting and using personal data that individuals may not reasonably expect.	Using fingerprint recognition technology to control access to a building.
9	Does the initiative involve the transfer of personal data outside of the European Union?	This relates to sending personal data to countries outside of the European Union.	Storing personal data in a cloud service hosted in the USA.
10	Does the initiative prevent individuals from exercising a right or using a service or contract?	This includes personal data processing that takes place in a public area that passers-by cannot avoid, or processing that aims to allow or refuse an indidvidual's access to a service.	Screening applicants before allowing them to use a web service.

3.2 Step Two - Describe the information flows

Record the following in the DPIA template:

- How personal data will be obtained
- How personal data will be processed (including potential future uses)
- How personal data will be stored
- To whom personal data will be disclosed (individuals or organisations, if any).

Consultation should begin during this step (see Consultation section beneath Step 6 below).

3.3 Step Three - Identify and assess the privacy risks

Record the identified risks in the DPIA template. This forms the core of the DPIA process. The aim is to compile a comprehensive list of all of the privacy risks associated with the initiative, whether or not the risks require action.

For each privacy risk identified, the following should be recorded:

- A unique identifier
- A description of the risk
- An assessment of the impact of the risk (severe, major, moderate, minor, insignificant)
- An assessment of the likelihood of the risk (very likely, likely, neither likely, nor unlikely, unlikely, very unlikely).

3.4 Step Four - Identify and approve the controls

Identify controls to mitigate the risks and record them in the DPIA template. The aim is to identify sufficient controls to eliminate each of the risks identified in Step Three, or to reduce them to a level which is acceptable to the Trust. For some identified risks, no controls may be required because the likelihood is so low and/or the impact so small that the risks are acceptable to the Trust.

Controls may take many forms, such as:

- Additional terms and conditions in a contract
- A privacy notice
- Documented operational procedures
- Disabling certain product features
- User training
- Technical controls, such as encryption.

Once a control is identified, the expected result of its implementation should be recorded i.e. whether it is likely to:

- Eliminate the risk
- Reduce the risk to an acceptable level
- Require acceptance as there is no reasonable control to eliminate or reduce it.

Proposed controls should then be approved by an appropriate individual. Normally this should be the Information Asset Owner or their nominated delegate, but it could also be:

- The project sponsor/manager
- The chair of a relevant committee.

3.5 Step Five - Assign responsibility for implementing controls

Allocate the controls to appropriate individuals and record an agreed deadline for implementation.

In the case of formal Trust projects, the implementation of many of the controls will fall within the scope of the project, so should be managed in the same way as any other project task. However, the implementation of some controls will be beyond the scope of the project (such as a change to Trust policy) so related tasks should be assigned through the Trust's normal management processes and added to the list of project dependencies. Where initiatives are being run informally, or as 'business as usual' activities, the Trust's normal management processes should be used to identify who will implement the controls and agree an appropriate deadline. In all cases, a named individual and deadline for completion should be assigned and recorded.

In the absence of formal project management documentation, the DPIA should be used to record when controls are implemented.

3.6 Step Six - Re-assess and accept the risks

After the controls have been implemented, re-assess the risks and record the outcome in the DPIA template. The risks then need to be accepted by an appropriate individual. Normally this should be the Information Asset Owner or their nominated delegate, but it could also be:

- The project sponsor/manager
- The chair of a relevant committee.

The individual who signs off the risks should have a clear understanding of the initiative, particularly the privacy risks and how the controls address them. If any risk has not been reduced to an acceptable level after implementation of the controls identified in Step Four, additional controls will need to be identified and Step Five and Step Six will need to be repeated.

Consultation

Consultation serves many purposes throughout the DPIA process, such as:

- Explaining the initiative to stakeholders
- Explaining to stakeholders how the DPIA process will be used within the initiative to manage privacy risks
- Establishing current working practices that the initiative aims to update or replace
- Establishing how the new system or process is likely to be used in practice and in the case of general purpose facilities, their likely purpose
- Establishing the privacy concerns of stakeholders

- Soliciting suggestions for controls
- Explaining identified controls to stakeholders.

Key stakeholders are likely to include:

- Individuals who understand the initiative from a technical point of view and in terms of personal data processing
- Individuals who will be using the new system or process
- Individuals whose personal data will be processed by the new system or process
- Collaborative partners
- The suppliers of a system
- The Trust's Data Protection Officer
- The Trust's Information Governance Manager, the ICT department and Legal Services.

3.7 Step Seven: How to conclude the DPIA

The following needs to be recorded:

- what additional measures are planned;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether the ICO needs to be consulted.

Every risk does not always have to be eliminated. It may be decided that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, the DPO will need to consult the ICO before the processing can go ahead.

As part of the sign-off process, advice should be sought from the DPO on whether the processing is compliant and can go ahead. If it is decided not to follow the DPO's advice, the reasons need to be recorded.

Any reasons for going against the views of individuals or other consultees should also be recorded.

In cases where the impact of a risk identified at Step Three is assessed to be either severe or major and likelihood is assessed to be either likely or very likely, the Trust's Data Protection Officer must be consulted without delay and before any processing begins. If any risk remains at this level after the implementation of controls, the DPO may be required to consult the Information Commissioner's Office.

A copy of the completed DPIA should be forwarded to the Information Governance Manager who will keep a central register and monitor progress against the actions.

4.0 Training Expectations for Staff

4.1 IAOs receive training in the use of DPIAs via the IAO half yearly workshops.

5.0 Implementation Plan

5.1 The latest ratified version of this procedure 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 procedure during Trust Induction.

6.0 Monitoring Compliance with this Procedure

6.1 The completion of DPIAs will be monitored by the DPO and IG Working Group who will receive an update on all DPIAs completed and outcome in the period since the last meeting.

7.0 Appendices

Appendix A – Data Protection Impact Assessment Template

DPIA author:	
Initiative title:	
Date completed:	

Context

Provide a brief explanation of the initiative - What is the initiative for? When is it likely to happen? How will it provide a benefit to the Trust? How will it provide a benefit to others?

Step One - Identify the need for a DPIA

Screening question	**Yes/No**
Does your initiative involve evaluating or scoring individuals (including profiling and predicting)?	
Does your initiative involve automated decision-making that may have a significant effect on an individual?	
Does your initiative involve systematic monitoring?	
Does your initiative involve the processing of sensitive personal data?	
Does your initiative involve processing personal data on a large scale?	
Does your initiative involve datasets that have been matched or combined?	
Does your initiative involve the personal data of vulnerable people?	
Does your initiative involve the use or application of innovative technological or organisational solutions?	
Does your initiative involve the transfer of personal data outside of the European Union?	
Does your initiative prevent individuals from exercising a right or using a service or contract?	

Based on the above information, it has been decided that a full DPIA [is/is not] required.

Step Two – Describe the information flows

Step Three – Identify and assess the privacy risks

Please tab to add more rows to the table if needed.

Risk ID	Privacy risk	Impact	Likelihood

Step Four - Identify and approve controls

Please tab to add more rows to the table if needed.

Risk ID	Control(s) identified	Expected result	Approved by

Step Five – Assign responsibility for implementing controls

Please tab to add more rows to the table if needed.

Risk ID	Control(s)	Responsible officer	Deadline for implementation	Completion date

Step Six – Reassess and accept the risks

Please tab to add more rows to the table if needed.

Risk ID	Privacy risk	Impact after control	Likelihood after control	Risk accepted by

Consultation

The conduct of this Data Protection Impact Assessment has involved the following consultation:

Step Seven - Sign off and record outcomes

Item	Name/Date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

Contact for raising additional privacy concerns

Name:			
Job title:			
Email address:		Telephone:	

Appendix F

Yorkshire Ambulance Service NHS
NHS Trust
An Aspirant Foundation Trust

Procedure for Handling Disclosure Requests under the General Data Protection Regulations 2016 and the Data Protection Act (2018)

Document Reference	PO – Procedure for Handling Disclosure Requests under the General Data Protection Regulations and Data Protection Act (2018) – November 2017
Version	V3.0
Responsible Committee	Trust Management Group
Responsible Director (title)	Steve Page, Executive Director of Quality, Governance and Performance Assurance/ Deputy Chief Executive
Document Author (title)	Caroline Balfour, Legal Services Manager
Approved By	Trust Management Group
Date Approved	
Review Date	
Equality Impact Assessed (EIA)	Yes
Protective Marking	Not protectively marked

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
2.0	April 2010	Angela Brown	A	Version produced and approved by the Information Governance Group.
2.1	August 2013	Caroline Balfour	D	Reformatted to be in line with policy and procedural documents template. Revision of content.
2.2	Oct 2015	Danielle Conway	D	Minor amendments Throughout.
3.0	Nov 2015	Caroline Balfour	A	Approved by TMG
3.1	April 2018	Allan Darby	D	Amendments to comply with the GDPR and DPA 2018
A = Approved D = Draft				
Document Author = Caroline Balfour, Legal Services Manager				
Associated Documentation: Data Protection Policy and Associated Procedures Information Governance Policy Information Governance Strategy				

1.0 Introduction

1.1 All requests for disclosure of person identifiable information (PII) are dealt with by the Legal Services Department. No such information must be disclosed outside the Trust unless it has been managed and approved by Legal Services in accordance with this Procedure and its processes. If any member of staff is approached for PII they must pass on the request to Legal Services at the earliest opportunity.

2.0 Purpose/Scope

2.1 The aim of this document is to outline the process to be followed in response to a request for disclosure under the General Data Protection Regulations (GDPR) and Data Protection Act 2018 ('the Act') which outlines rights of access to PII.

2.2 The procedure should be read in conjunction with the Data Protection Policy, which outlines the principles of the GDPR and Act 2018.

3.0 Requests for Personal Identifiable Information – general staff information and guidance

3.1 Under Article 15 of the GDPR, subject to certain conditions and exemptions, there is an entitlement to apply for access to personal data known as a 'subject access request' ("SAR"). Under the Regulations the request must be complied with within one month of receipt, although this time may be extended by a maximum of two calendar months for complex requests.

3.2 Most of the requests for PII made to the Trust are for health records and patient information. A health record is defined in the Act as any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual. These records are classed under the Act as special categories of data. The Act gives rights of access to every living person, or their authorised representative, to apply for their health records irrespective of when the records were compiled.

3.3 Subject access requests can also be for non-health related records e.g. personnel file, references, emails etc.

3.4 The Access to Health Records Act 1990 governs access to the health records of deceased people.

3.5 The Access to Medical Reports Act 1988 governs access to medical reports made by a patient's normal clinician for insurance or employment purposes.

3.6 All requests for such disclosures must immediately be sent to the Trust's Legal Services Department at the email address: subjectaccessrequests@yas.nhs.uk. Telephone advice is available from the Legal Services Team.

4.0 Requests for Personal Identifiable Information - Legal Services Department procedure for subject access requests

4.1 The Trust's Legal Services Department responds to requests for records from patients, their personal representatives, litigation friends, lawyers or parents. It is important to note that the right of access to personal data is that of the data subject

alone. Therefore, before disclosing any records to anyone other than the patient (i.e.

to a third party), the Trust must be satisfied that the patient has consented that the disclosure should be made to the third party.

4.2 On receipt of a request the Legal Services Department will contact the requestor to clarify the details of the request, request proof of identification or written consent for release and request the relevant fee. This information is prompted by use of standard forms (Appendix A). The Legal Services Department centrally holds a library of template letters for correspondence and these have been approved by the Legal Services Manager.

4.3 All Subject Access Requests (SARs) must be made in writing and information must normally be provided free of charge in response to a subject access request. However, a charge may be made if the request is 'manifestly unfounded or excessive' and there may be a reasonable charge for further copies requested.

4.4 The obligation to comply with a subject access request takes effect once the Trust has the information necessary to identify the applicant and locate the information and the fee where relevant. In exceptional circumstances if it is not possible to comply within the time limit, the applicant will be informed. The dates that the obligation arises and is completed are recorded on a central spreadsheet by the Legal Services Department. Key Performance Indicators for completion of the request are monitored monthly and form part of the Trust's Integrated Performance Report.

4.5 Proof of identification is checked by having sight of photographic identification e.g. passport, driving licence and separate proof of address e.g. utility bill. Consent for release to a third party is required to be in writing and specific. These are initially requested and checked by the Legal Services Assistant .

4.6 The Legal Services Department will access the relevant databases and files to collate the data requested relating to the subject and prepare documents for disclosure. This is likely to involve the redaction of third party details under the Act as incident logs record vehicle positions which may be addresses of other individuals. This is done electronically.

4.7 The Legal Services Department will keep individual electronic files for each subject access request and all documentation will be scanned and saved. Electronic copies of prepared disclosure documents should be saved in a disclosure subfolder.

4.8 Prior to disclosure, the disclosure bundle, consent and proof of identification will be quality checked by the Legal Services Manager or an appropriate deputy.

4.9 The disclosure bundles are posted out by recorded delivery with a closure cover letter.

4.10 If the requestor is unhappy with the way in which his/her request has been treated they can contact the Legal Services Department in the first instance, with escalation to the Legal Services Manager and the Data Protection Officer. Requestors are also informed of their right to contact the Information Commissioners Office (ICO) if they have any concerns with the way in which their request has been handled in addition to providing the details regarding their other rights as a data subject (see section 3.4 of the Data Protection Policy).

5.0 Requests for Personal Identifiable Information - Specific circumstances

5.1 Access to Records of Children

5.1.1 As a general rule, a person with parental responsibility will have the right to apply for access to a health record for a child under 13. The Legal Services Assistants will seek to verify this prior to disclosure.

5.1.2 Patients aged 16 and over are regarded as adults in law for the purposes of consent to treatment and right to confidentiality and they may, therefore, consent to or refuse disclosure of their records to a third party, including their parents. Children under 16, who are deemed to have sufficient understanding to consent to, or to refuse proposed treatment, or a request for disclosure, are entitled to decide and to have their confidence respected. Good practice dictates that the child should be encouraged to involve parents, or other legal guardians, in decisions on treatment or disclosure.

5.2 Access to Records of Adults without Capacity

5.2.1 For patients, who because of their mental or physical condition, are unable to give consent to disclosure of their health records, the decision on whether or not to disclose will be made in the patient's best interests by the patient's treating doctor and the Trust's Executive Medical Director. The views of families and carers will inform that decision.

5.2.2 A person appointed by the court to manage affairs on behalf of an incapacitated patient has a right under the DPA to receive information about that patient. This will be a person who holds a Lasting Power of Attorney for the data subject or a deputy appointed by the Court of Protection.

5.3 Access to Records of Deceased People

5.3.1 Health records relating to deceased people do not carry a common law duty of confidentiality. However, it is Department of Health and General Medical Council policy that records relating to deceased people should be treated with the same level of confidentiality, as those relating to living people. Access to the health records of a deceased person is governed by the Access to Health Records Act 1990. Under this legislation, when a patient has died, their personal representative or executor or administrator, or anyone having a claim resulting from the death (this could be a relative or another person), has the right to apply for access to the deceased's health records. These facts are verified by the Legal Services Administrators prior to disclosure.

5.4 Requests for audio recordings

Transcripts of calls, with all third party information redacted, may be disclosed with the authorisation of the Legal Services Manager and audio recordings of calls may be disclosed at the discretion of the Legal Services Manager. A declaration limiting use of the audio recording must be agreed and signed and returned by the requestor prior to disclosure (See Appendix B)

6.0 Disclosure Requests from the Police

6.1 There is an exemption in the DPA to non-disclosure (i.e. that allows the disclosure) of person identifiable information for the purposes of crime and taxation (Schedule 2 para 2 and 3 of DPA 2018). In respect of crime, the effect of Schedule 2 is that where personal data is being processed for the prevention or detection of crime, or for the

apprehension or

prosecution of offenders, then the requirements for fair and lawful processing can be dispensed with.

6.2 The exemption does not cover the disclosure of all personal information in all circumstances. Information may be disclosed to the police only if it cannot be obtained from another source, if it is the minimum necessary for the stated purposes and not merely convenient, and if not releasing it would be likely to prejudice (i.e. significantly harm) any attempt by the police to prevent crime or to catch a suspect. Under these circumstances, it is not necessary to obtain the consent of the data subject. The purpose of Schedule 2 is to allow disclosure without informing the data subject, where giving that notification might prejudice the police investigation for the prevention of crime or catching a suspect. This is subject to the Department of Health guidance detailed in 6.6 below.

6.3 Police requests for information must be passed to the Legal Services Department via the email address: policerequests@yas.nhs.uk.

6.4 The request must either be made in writing, or if made by telephone must be confirmed in writing, on a Request for Disclosure of Personal Data / Schedule 2 Request form, counter signed by a senior police officer, ideally of Inspector rank or above.

6.5 If a Request for Disclosure of Personal Data / Schedule 2 Request form is not forthcoming then the Trust will not at that stage comply with the disclosure request unless a section of the Data Protection Act is appropriately relied upon. In this instance the request will also have to be in writing. The exception to this is if the circumstances are such that information is required immediately and an undertaking is given to provide retrospective documentation.

6.6 The Legal Services will determine if the Schedule 2 provision is appropriate in line with Department of Health guidance on severity of offence and threshold for release. In order to justify disclosure, the circumstances of the matter must be sufficiently serious that the substantial public interest in disclosure outweighs any duty of confidence owed to the data subject.

6.7 The Legal Services Assistants will record the request on the centrally held Police requests spreadsheet and create an electronic file for each request, scanning and saving all correspondence and disclosures. The Legal Services Department will access the data requested, prepare documents for disclosure and complete the request, noting the completion date for key performance indicator analysis. This is monitored monthly and forms part of the Trust's Integrated Performance Report.

6.8 A fee will not be charged when providing records to the police for the prevention or detection of crime, or for the apprehension or prosecution of offenders.

7.0 Out Of Hours Disclosure

7.1 It is not the policy of the Trust to disclose data relating to any patient or member of staff outside standard working hours (Mon to Fri, 8am to 4pm, except Bank Holidays) and any requests for disclosure received after 4pm will normally be processed the next working day.

7.2 Emergency requests, predominantly from the police, may arise out of hours and in this instance the request is handled by the Emergency Operations Centre in accordance with the Out of Hours Procedure (Appendix C)

7.3 Emergency requests that are received in the NHS 111 service out of hours are handled by the NHS 111 team in accordance with the Out of Hours Procedure (Appendix D)

8.0 Limitations on Access to Records

8.1 Under the DPA, there are only two reasons why access can be denied or limited to a patient, or their authorised representative:

a) Where the data controller judges that the information disclosed may cause serious harm to the physical or mental health or condition of the patient, or any other person.
b) Where giving access would disclose information relating to or provided by a third person who had not consented to that disclosure, unless it is reasonable in all the circumstances to comply with the request without the consent of the third party individual. The Legal Services Manager will make the decision on disclosure under this exemption.

8.2 Where consent of a third party is not satisfied, information should still be disclosed without revealing the identity of the third party, for example, by redaction, such that the resulting information is genuinely anonymous.

8.3 Healthcare professionals who have compiled or contributed to the health records, or who have been involved in the care of the patient, are not exempt from disclosure of third party information about themselves.

8.4 Requests by people with parental responsibility can be denied if the child gave the information contained in their records with the express wish, or in the expectation that it would not be disclosed to their parents.

8.5 Under the Access to Health Records Act 1990, if the deceased person had indicated that they did not wish information to be disclosed, or if the record contains information that the deceased person expected to remain confidential, then it must remain so. The same limitations on serious harm to mental or physical health and to the identification of a third person, which affect disclosure under the DPA, apply equally to the records of deceased people.

9.0 Disclosure without Consent

9.1 Occasionally it will be necessary to disclose a patient's records without their consent and, rarely, in contradiction of the patient's clear objection to disclosure. There are three possible justifications for this:

a) If it is believed that a patient may be a victim of neglect or abuse, and that they lack capacity to consent to disclosure and that disclosure is in the patient's best interests.
b) If you believe that it is in the wider public interest, or that it is necessary to protect the patient, or someone else, from the risk of death or serious harm. (examples of this might be to inform the DVLA if someone may be unfit to drive, in addition to disclosure to assist the police in preventing or solving a serious crime or informing the police if you have good reason to believe that a patient is a threat to others).
c) Disclosure is required by law (for example, in accordance with a statutory obligation, or to comply with a court order or a disclosure notice from the NHS Counter-Fraud Service).

In any of these cases, the Trust should only provide the minimum amount of information necessary to serve the purpose, and the designated member of staff

processing the request should carefully document the reasons for making the disclosure, as approved by the Legal Services Manager or an appropriate senior manager. Advice should be sought from the Legal Services Team.

10.0 Training Expectations for Staff

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

11.0 Implementation Plan

11.1 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 guidance during Trust Induction.

12.0 Monitoring Compliance with this Procedure

12.1 The Trust's Integrated Performance Report will be monitored by the Trust Board in respect of key performance indicators relating to compliance with subject access requests.

12.2 Also via the Integrated Performance Report the Trust Board will monitor to ensure that no Data Protection Act undertakings, enforcement notices, 'stop now' orders, compulsory assessment notices or monetary penalty notices are served on the organisation by the Information Commissioners Office.

12.3 Information Governance incidents will be monitored by both the Clinical Governance Group and the Information Governance Working Group.

13.0 References

- Great Britain. 1990. Access to Health Records Act 1990. *Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. Access to Medical Reports Act 1998. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *GDPR and Data Protection Act 2018*. London: HMSO. Available at: www.legislation.gov.uk
- The Data Protection (Subject Access Modification) (Health) Order 2000. SI 2000 No.413
- NHS Information Governance: Guidance on Legal and Professional Obligations September 2007
- Frequently asked questions about accessing health records: Department of Health www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentiality andcaldicottguardians/DH
- Guidance for Access to Health Records Requests. DH February 2010
- Guidance for Access to Health Records Requests under the GDPR and Data Protection Act 2018. DH Version 2 June 2003
- Use and Disclosure of Health Data: Guidance on the application of the GDPR and Data Protection Act 2018. ICO May 2002. www.ico.gov.uk

- Data Protection Act Legal Guidance. Information Commissioner's Office (ICO) http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf
- Data Protection Technical Guidance Note: Dealing with subject access requests involving other people's information. ICO. www.ico.gov.uk
- Data Protection Technical Guidance: Subject access requests and legal proceedings. ICO. www.ico.gov.uk
- Data Protection Good Practice Note: Checklist for handling requests for personal information (subject access requests). ICO. www.ico.gov.uk
- Data Protection Good Practice Note: Releasing information to prevent or detect crime. ICO. www.ico.gov.uk
- Subject access to health records. GDPR and Data Protection Act 2018, Compliance advice. ICO
- London Ambulance Service Policy for Access to Health Records, Disclosure of Patient Information: Protection and Use of Patient Information
- Medical Protection Society (MPS) Updated: Access to health records January 2010.

Appendix A1: Subject Access Request form – Health Records
http://pulse.yas.nhs.uk/StaffHandbook/Legal%20Service%20Documents/SUBJECT%20ACCESS%20REQUEST%20FORM%20(PDF).pdf

Appendix A2: Subject Access Request form – Personal data (excluding health records)

http://pulse.yas.nhs.uk/StaffHandbook/Legal%20Service%20Documents/HR%20SUBJECT%20ACCESS%20REQUEST%20FORM%20(PDF).pdf

Appendix B: Declaration form for Subject Access Requests for audio recordings

http://pulse.yas.nhs.uk/StaffHandbook/Legal%20Service%20Documents/AUDIO%20DECLARATION%20FORM%20(PDF).pdf

Appendix C: Emergency Operations Centre emergency police disclosure (Out of Hours Procedure)

http://pulse.yas.nhs.uk/StaffHandbook/Legal%20Service%20Documents/Emergency%20Operations%20Centre%20-%20Police%20Requests.pdf

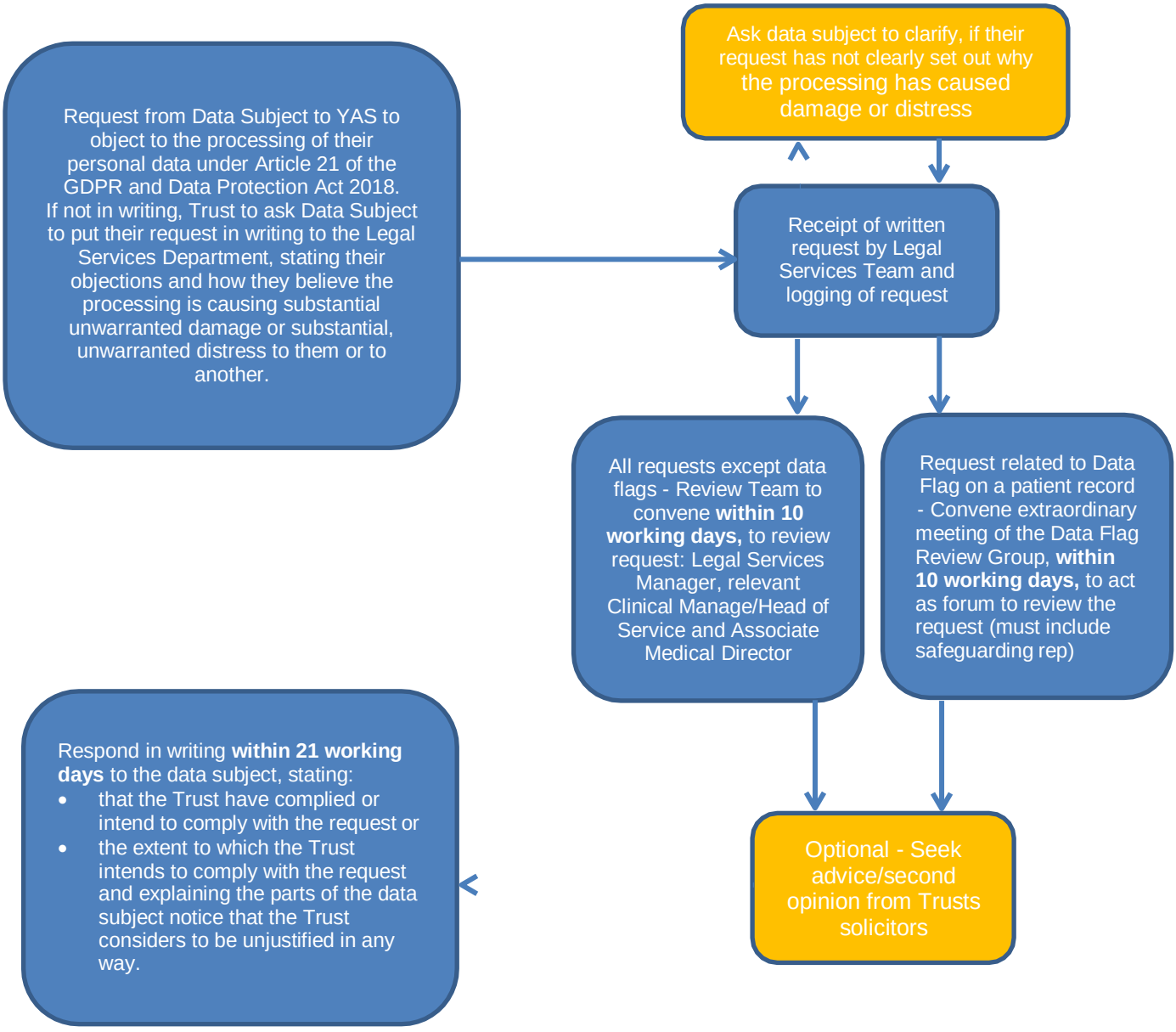
http://pulse.yas.nhs.uk/StaffHandbook/Legal%20Service%20Documents/EOC%20Emergency%20Disclosure%20of%20Information%20to%20Police%20-%20Out%20of%20Hours%20Checklist.pdf

Appendix D: NHS 111 emergency police disclosure (Out of Hours Procedure)

http://pulse.yas.nhs.uk/StaffHandbook/Legal%20Service%20Documents/8.7%20NHS%20111%20Emergency%20Police%20Disclosure%20v2.pdf

Appendix G

Process Flow Chart – Handling Article 21- Right to Object Notices under the GDPR and Data Protection Act 2018



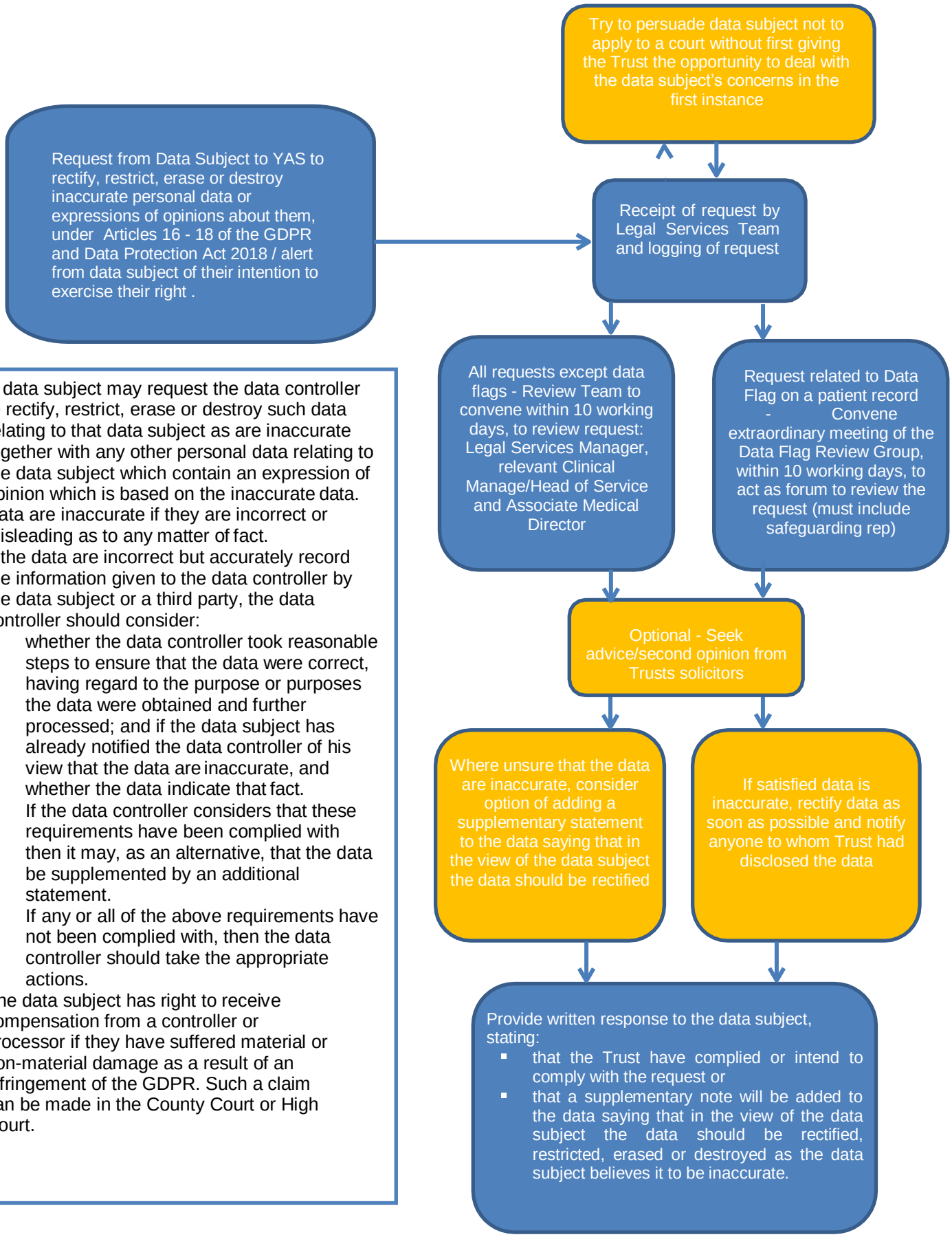
An individual has no right to object to processing if their personal data is required for:

- The performance of a task in the public interest by an official authority.
- Direct marketing (including profiling).
- Historical or scientific research.

How to recognise an Article 21 request:

- It is important to remember that an Article 21 request may not be easily recognisable.
- It may not mention Article 15 and may form part of a lengthy piece of correspondence.
- It doesn't have to be and in most case won't be, in the form of any formal notice. For example it could be a complainant asking for all his case documents to be deleted or destroyed, albeit the Regulation refers to processing not deletion.

Process Flow Chart – Handling Notices under Articles 16 – 18 of the GDPR and Data Protection Act 2018 (Dealing with Inaccuracy)



- A data subject may request the data controller to rectify, restrict, erase or destroy such data relating to that data subject as are inaccurate together with any other personal data relating to the data subject which contain an expression of opinion which is based on the inaccurate data.
- Data are inaccurate if they are incorrect or misleading as to any matter of fact.
- If the data are incorrect but accurately record the information given to the data controller by the data subject or a third party, the data controller should consider:
  - whether the data controller took reasonable steps to ensure that the data were correct, having regard to the purpose or purposes the data were obtained and further processed; and if the data subject has already notified the data controller of his view that the data are inaccurate, and whether the data indicate that fact.
  - If the data controller considers that these requirements have been complied with then it may, as an alternative, that the data be supplemented by an additional statement.
  - If any or all of the above requirements have not been complied with, then the data controller should take the appropriate actions.
- The data subject has right to receive compensation from a controller or processor if they have suffered material or non-material damage as a result of an infringement of the GDPR. Such a claim can be made in the County Court or High Court.