# POL2/87 – Confidentiality and Data Protection

NHS Blood and Transplant

**Copy No:**
**Effective date: ~~07/12/25~~**

## Changes in this version

Updated to Version 8 to incorporate statutory reforms under the Data (Use and Access) Act 2025 (DUAA), mandatory pre-deployment governance standards for Artificial Intelligence (AI) and algorithmic decision-making, perimeter privacy restrictions for wearable recording technologies (smart glasses), SIRO oversight for management access to employee mailboxes, and the statutory transition to the Information Commission. Incorporates reference to the UK Government Algorithmic Transparency Recording Standard (ATRS) within the AI and algorithmic governance framework, as recommended by the Audit, Risk and Governance Committee (ARGC).

**Commented [AO1]:** Alignment with Cover Paper Executive Summary & Purpose. Reflects formal transition to the Information Commission and incorporates DUAA 2025 statutory reforms.

## Policy

**Formatted:** Font: 12 pt

NHS Blood and Transplant (NHSBT) will develop, implement and maintain technical and organisational measures to protect the privacy of all individuals, living or deceased, about whom it holds information. It will achieve and maintain compliance with all applicable common law and statutory requirements, and sector best practice. These include but are not limited to the UK General Data Protection Regulation, Data Protection Act 2018, Data Use and Access Act 2025, Privacy and Electronic Regulations 2003, the Access to Health Records Act 1990, the NHS Confidentiality Code of Practice, and the reports of the National Data Guardian

## Purpose

**Formatted:** Font: 12 pt

**Formatted:** Font: 12 pt

This document outlines the responsibilities, processes and procedures in place to ensure that the privacy and confidentiality of donors, patients, employees and other supporters of NHSBT are respected and maintained

## Responsibilities

**Formatted:** Font: 12 pt

Responsibility for compliance with this policy exists at all levels throughout NHSBT but legal accountability rests with the Chief Executive. Specific responsibilities are delegated to groups or posts as detailed within this policy, POL266 NHSBT's overarching Data Security, Privacy and Records Management policy, and related documents.

~~The Data Protection Officer is responsible for maintaining NHSBT's notification to the Information Commissioner's Office (ICO), as required under the Data Protection Act 2018.~~

The Data Protection Officer is responsible for maintaining NHSBT's notification to the **Information Commission**, as required under statutory data protection legislation.

**Commented [AO2]:** Terminology consistently across the policy, replacing legacy references to the "Information Commissioner's Office".

The Information Governance Committee (IGC) is responsible for review and approval of this policy

# POL2/8~~7~~ – Confidentiality and Data Protection

**Copy No:**
**Effective date:** ~~07/12/25~~

## Introduction

~~NHS Blood and Transplant (NHSBT) is a Special Health Authority within the NHS. It manages the national voluntary donation system for blood, tissues, organs and stem cells turning these precious donations into products that can be used safely to the benefit of the patient. It also provides a range of specialist laboratory services.~~

NHS Blood and Transplant (NHSBT) is an executive arm's length public body of the Department of Health and Social Care, constituted as a Special Health Authority. It manages the national voluntary donation system for blood, tissues, organs and stem cells, turning donations into therapeutic products that can be safely administered to patients. Its statutory remit includes looking after blood donation services in England, transplant services across the United Kingdom, delivering specialist diagnostic and laboratory services, and researching new treatments and clinical processes.

**Commented [AO3]:** Aligns with Cover Paper Section 2 (Item 1: Legal Status & Scope). Standardises NHSBT's formal definition as an executive arm's length Special Health Authority across all commercial and regulatory frameworks.

As part of its operations, NHSBT must collect, hold, use and create information about identifiable individuals. When such individuals are living, NHSBT must observe its obligations and the individuals' rights under the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and the Data Use and Access Act 2025. Common law duties of confidentiality also apply, as in the exchange of information between donor and healthcare professional. Such duties are held to apply even after the death of the individual, and so it is important that similar standards of protection are maintained for information about deceased persons.

## Scope

This policy applies to all collection, use, holding, sharing and disposal of person-identifiable data by or on behalf of NHSBT, irrespective of the information system used. This includes, but is not limited to, the processing of personal data as defined by UK GDPR. Where the term "Service" is used, this will be taken to mean the whole of NHSBT. Any exceptions will be explicitly stated.

The policy is to be observed by:

- All full time and part time employees of NHSBT, in all its functions and departments
- The Chairman, Executive and Non-Executive members of the NHSBT Board,
- The NHSBT Executive,

contracted third parties working under the direction of NHSBT, at any location worldwide, be that an official NHSBT site or any other location where NHSBT work is carried out.

This policy applies irrespective of the format of the information. This includes all media such as: paper, printouts, email, fax, databases, portable devices, tapes, discs, audio recordings, microfilm and CDs. It also covers verbal exchange of personal data.

## Terminology

A glossary of terms used in this document and throughout Data Protection legislation and guidance is included as Appendix 2.

**Policy**

NHSBT must respect and protect the privacy of all individuals, be they donors, patients, employees or other supporters, with whose information is entrusted. Gaining and maintaining the trust of stakeholders is crucial to its success in recruiting and retaining donors, and in winning and retaining customers for its products and services.

Protection of privacy is secondary, the provision of safe care to donors and patients is paramount. For this reason, full and correct details must be collected and used for identification of donors and patients, in the donation supply chain and the delivery of direct care.

Privacy is to be protected by restricting access to personal data on a 'need to know' basis. Irrespective of their compliance with duties of confidentiality, if employees can access more detail than they need for their jobs this will be regarded as a breach of policy. For any task which involves the use of personal or special category data every effort should be made to use the minimum amount of data necessary for the purpose and comply with the principles of data minimisation. Where possible, and where there would not be a clinical risk, data should be anonymised, or if that is not possible, pseudonymised.

Confidentiality and Data Protection are part of a wider Data Privacy and Data Security agenda that seeks to ensure the confidentiality, integrity and availability of NHSBT's information assets. DSPR is responsible for facilitating the Information Asset Register. This is described in NHSBT's Data Security, Privacy and Records Management Policy, POL266.

**The Caldicott Principles and the National Data Guardian (NDG)**

NHSBT will promote and comply with the Eight Caldicott Principles established by the committees chaired by Dr Nicola Byrne, the National Data Guardian for Health and Social Care (NDG) advising on the use and protection of patient information across the NHS, namely:

**Principle 1**: Justify the purpose(s) for using confidential information.
**Principle 2**: Use confidential information only when it is necessary.
**Principle 3**: Use the minimum necessary confidential information.
**Principle 4**: Access to confidential information should be on a strict need-to-know basis.
**Principle 5**: Everyone with access to confidential information should be aware of their responsibilities.
**Principle 6**: Comply with the law.
**Principle 7**: The duty to share information for individual care is as important as the duty to protect patient confidentiality.
**Principle 8**: Inform patients and service users about how their confidential information is used.

NHSBT recognises that the Caldicott Principles are consistent with yet secondary to its statutory and common law obligations, as underlined by Caldicott Principle 6 – 8 NHSBT's interpretation of Caldicott Principle 7 is that it will support the sharing of personal confidential information with third parties when the sharing is for the benefit of a patient, donor or associated third party, is necessary for and proportionate to the achievement of that benefit and is done in such a way as to balance the need for prompt availability with the risks of the method chosen.

The National Data Guardian (NDG) is an independent champion for patients and the public when it comes to matters of their confidential health and care information. The NDG advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used appropriately in line with the guidance from the Caldicott Council. The UK Caldicott Guardian Council (UKCGC) is the national body for Caldicott Guardians and a sub-group of the National Data Guardian Panel.

The National Data Guardian (NDG) is an independent advisor to the government and the health and adult social care system in England. They help ensure that confidential health and social care data is handled safely and used in ways that people expect and can trust. The NDG is not a regulator with investigative powers. Instead, they provide advice and guidance that shapes data policy, practice and IT programmes, helping the system use data responsibly to support and improve people's care, health service planning, and innovation and research.

The NGD key areas include::

- **Improving access to healthcare information**

Formatted: Font: 12 pt

- **Developing strong guidance and policy**
- **Advising on transparency and engagement to strengthen trust**
- **Promoting the Caldicott Principles and supporting Caldicott Guardians**

Compliance with the NDG recommendations and reviews is reflected in the Caldicott Guardian checklist as part of the Data Protection Impact Assessments (DPIAs)

**Information Sharing**

NHSBT endorses the sharing of information with third parties where this supports the interests of patients, donors, the public or itself. Any sharing must be within the law, and supported by:

- a documented procedure for routine sharing.
- a formal contract aligned to Article 28 GDPR,
- a data processing impact assessment (DPIA)
- a documented data sharing agreement that includes the purposes, limits, methods and obligations of parties, or
- a record of the factors considered in deciding whether to share information in response to a non-standard request. that could not be covered by any of the previous bulleted items, a record of this decision must be sent to the DSPR team to log.
- A security due diligence done on the third party with the help of the FRM5280 form.
- Data processing agreements and relevant assurances in place for any third-party processors.

The necessary level of authority for routine sharing of information will be defined in procedure documents. Non-routine disclosures must be authorised by the Information Asset Owner. The approval of the Caldicott Guardian or one of their delegated authorities (the Associate Medical Directors), must be obtained for non-routine disclosure of person-identifiable clinical details, for example to law enforcement agencies. If in doubt, the advice of the Data Security, Privacy and Records Management - DSPR Team should be sought.

**Management Access to Employee Mailboxes**
Access to current or former employee email accounts without the mailbox holder's explicit consent is strictly prohibited, save in exceptional circumstances. Any non-consensual mailbox inspection must demonstrate clear operational necessity, undergo formal Data Privacy review, and receive prior written authorisation from the Senior Information Risk Owner (SIRO). Unilateral or unapproved management access will be treated as a serious security breach and investigated under NHSBT's Disciplinary Policy.

**Commented [AO4]:** Aligns with Cover Paper Section 2 & Detailed Operational Implications (Item 2: Management Email Access). Codifies strict SIRO sign-off governance, eliminating historical ambiguity around accessing staff/leaver mailboxes.

**Lawful Basis for Processing**

The Data Use and Access Act 2025 (DUAA) will not replace the UK General Data Protection Regulation ("UK GDPR"), Data Protection Act 2018 or the Privacy and Electronic Communications (EC Directive) Regulations 2003, but it will make some changes to them to make the rules simpler for organisations, encourage innovation, help law enforcement agencies to tackle crime and allow responsible data-sharing while maintaining high data protection standards.

- **Automated decision-making (ADM)**
  The DUAA creates a more permissive framework under the UK GDPR for organisations to make decisions based solely on automated processing that

have legal or similarly significant effects on individuals. Organisations will be able to make such decisions in wider circumstances but must implement certain safeguards. These include:

- providing people with information about significant decisions made about them
- enabling them to make representations about and to challenge such decisions
- and enabling them to obtain human intervention in respect of such decisions

- **Subject Access**

  The DUAA clarifies the time limits for organisations to respond to subject access requests (requests by individuals to access and receive a copy of their personal data). It includes a "stop the clock" rule, allowing organisations to pause the response time if they need more information from the requester. Once they get the information they need, the response time continues. Organisations need to make **reasonable and proportionate** searches when responding to requests.

- **Children's Data Protection**

  New rules require certain online services likely to be accessed by children to consider how to protect and support them when designing these services.

- **Scientific Research**

  ~~The DUAA clarifies that scientific research may include commercial research. It allows researchers to seek consent for broad areas of related research and clearly outlines the safeguards required for using personal data in research.~~

  Under UK GDPR Article 4 (as amended by DUAA 2025), scientific research includes fundamental, applied, and commercially funded research carried out in the public interest, including technological demonstration and public health studies. NHSBT may seek broad consent for related research areas where specific project outcomes cannot be fully predetermined at the outset, provided appropriate technical, organisational, and ethical safeguards are documented.

- **Recognised Legitimate Interests**

  ~~The Act introduces a new lawful ground for processing personal data, giving businesses more confidence to use data for crime prevention, safeguarding, responding to emergencies, and other specified legitimate interests. This allows non-public bodies to process personal data for specific purposes (e.g. safeguarding, national security, public health) without conducting a full legitimate interests assessment. An example of Organisations that NHSBT works with that use this Legal basis is the collaborative work we do when~~

**Formatted:** Indent: Left: 1.27 cm

**Commented [AO5]:** Aligns with Cover Paper Section 2 (Item 3: Research & Legitimate Interests). Integrates DUAA 2025 provisions allowing broad consent for research and enabling collaborative university/commercial partners to rely on Recognised Legitimate Interests without separate LIAs.

~~conducting research. Universities would fall under this legal basis for their processing obligations.~~

DUAA 2025 establishes statutory recognised legitimate interests for non-public bodies collaborating with NHSBT (e.g., commercial research partners or universities), permitting data processing for specified purposes—including public health protection, responding to emergencies, and safeguarding vulnerable individuals—without the requirement to conduct a separate Legitimate Interests Assessment (LIA). NHSBT itself, as a public authority, continues to rely primarily on Public Task (Article 6(1)(e)) and Health/Social Care Management (Article 9(2)(h)) for its official functions.

- **International Data Transfers**

~~The Act simplifies the rules and provides necessary clarification for transferring personal data internationally.~~

Personal data must not be transferred outside the United Kingdom unless an approved transfer mechanism is in place. Where transfers involve countries or organizations lacking UK adequacy regulations, transfers must satisfy the statutory **Data Protection Test** (verifying that the standard of data protection is not materially lower than UK GDPR and DPA 2018) and be supported by an approved International Data Transfer Assessment.

**Privacy and Electronic Communications Regulations (PECR)**
In accordance with statutory updates, maximum financial penalties for serious PECR breaches align with UK GDPR standards (up to £17.5 million or 4% of global turnover). Digital services may deploy low-risk cookies without prior consent solely for essential functionality, service improvement analytics, or emergency location tracking, provided clear opt-out mechanisms and transparency notices are maintained.

- ~~**Responding to Complaints**~~

~~The DUAA requires organisations to handle complaints from individuals who are concerned that the way their information is used breaches the data protection legislation, for example by providing an electronic complaint form, and informing the individual about the outcome of a complaint.~~

**Data Protection Complaints Handling**
NHSBT maintains a defined public procedure for receiving and resolving complaints from individuals regarding the handling of their personal data. In accordance with DUAA 2025 standards, NHSBT will:

1. Formally acknowledge receipt of data protection complaints within **30 calendar days**;
2. Conduct appropriate enquiries without undue delay and keep the complainant informed of progress;

**Formatted:** Indent: Left: 1.27 cm

**Commented [AO6]:** Aligns with Cover Paper Section 2 & Risk Assessment (Item 4: International Data Transfers & PECR). Incorporates the statutory "Data Protection Test" and reflects the revised PECR penalty ceiling aligning with UK GDPR turnover maximums.

**Formatted:** Indent: Left: 1.27 cm

**Formatted:** Indent: Left: 1.27 cm

**Formatted:** Indent: Left: 1.27 cm

**Formatted:** Indent: Left: 1.9 cm, Tab stops: 2.54 cm, List tab + Not at 1.27 cm

3. Provide written notification of the substantive outcome and available escalation routes to the Information Commission.

**Commented [AO7]:** Aligns with Cover Paper Section 2 (Item 5: Statutory Complaints Handling). Translates the mandatory DUAA 2025 30-day acknowledgment requirement into an enforceable operational standard.

- **Storage and Access Technologies (such as cookies)**

  The Act allows the use of storage and access technologies without explicit consent in certain, low-risk situations.

Further guidance around the impact of the DUAA will be available ~~from the Information Commissioner's Office in 2026.~~from the Information Commission in 2026.

(Ref: Data (Use and Access) Act 2025: data protection and privacy changes - GOV.UK)

**Formatted:** Font: 12 pt

**Formatted:** Font: (Default) Arial

**Formatted:** Font: 12 pt

Under GDPR (Article 6) all information processing must have an identified legal basis to ensure that the processing is fair, lawful, and justified. These legal conditions need to be identified and communicated to donors, recipients, staff, or anyone whose data NHSBT is processing.

For Special Category (formally known as Sensitive Data) you must have at least one lawful basis under Article 6 and Article 9 of the UK GDPR.

The vast majority of NHSBT data processing will fall under Article 6(e)

*"Processing 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"*

AND

Article 9(2)(h)
*(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

To support choosing the correct lawful basis for data processing use the flow chart in appendix 1 or seek advice from the Data Security, Privacy and Records Management Team – (DSPR)

**Training and Awareness**

NHSBT will provide training in confidentiality and data protection within its programme of Data Security, Privacy and Records Management DSPR training. Please see POL209.

**Compliance and Assurance**

Compliance with this policy will be checked by inclusion of audit items in the specification for national and local self-inspections. Key components will be covered by licensing authorities during their inspection visits. Additional compliance checks and audits, both internal and external, will be performed on an ad hoc basis.

**Innovations, Changes and Existing Processes**

All changes and developments that impact any information asset and may lead to high risk to the rights and freedoms of individuals must undergo a Data Protection Impact Assessment (DPIA). This is a legal requirement in the UK GDPR and is the responsibility of the Information Asset Owner to ensure the DPIA process is followed. This applies to all service changes and innovations, whether or not managed by the Programme Management Office. See MPD1655.

Process owners are responsible for ensuring that appropriate privacy-protecting measures are included in all procedures and work instructions, and that these measures are reviewed and updated as necessary, in consultation with the Information Asset Owner(s).

**Person Identifiable Data (PID) and Pseudo-anonymisation**

NHSBT will comply with the definition of PID provided by NHS England Care must be taken to assess the data items both singly and in combination, to establish the degree to which they may identify individuals.

- name
- address
- date of birth or age
- gender
- sex
- NHS number or hospital record number
- telephone number
- email address
- marital status
- health information, including information about their symptoms, medical conditions, diagnosis, medication and treatment
- race and/or ethnicity
- religious and/or other beliefs
- sexual life and/or sexual orientation (where this is relevant to their care)
- living arrangements, living habits and diet
- genetic information

(Ref: https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/security-privacy/nhs-fdp-information-governance-framework/categories-of-personal-data/)

Formatted: Font: 12 pt

At all times measures are to be applied where necessary to prevent identification and protect privacy. These may include aggregation of low-number statistics, removal of all identifiers, or partial editing of data e.g., provision of partial dates of birth, partial postcodes. Details of appropriate techniques are ~~published by the Office for National Statistics and the Information Commissioner's Office.~~ published by the Office for National Statistics and the Information Commission.

**Enforcement**

~~Breach of this policy, whether knowingly or not, will be regarded as serious and will be managed under NHSBT's disciplinary policy. Applicable sanctions include dismissal, and/or referral to the criminal justice system or professional bodies.~~

Breach of this policy, whether knowingly or not, will be regarded as serious and will be managed under NHSBT's disciplinary policy. Applicable sanctions include dismissal, and/or referral to the criminal justice system or professional bodies.

**Specific Requirements of the General Data Protection Regulation**

Information and guidance about the GDPR are available ~~from the Information Commissioner's website at ICO.org.uk.~~ from the **Information Commission's** website at ICO.org.uk.
Article 5 of the GDPR sets out seven key principles which lie at the heart of the General Data Protection regime:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Article 5(1) requires that personal data shall be:

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

For each information asset the lawful basis for processing data must be identified and recorded, the flow chart in Appendix 1 can be used to support a decision on which is the most appropriate basis.

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

When collecting data from any individual it must be established and explained to the individual the purpose of the data collection and how it is going to be used, most is covered in the NHSBT public privacy notice. Should there be a need to use the data for other purposes post collection the Information Asset owner must follow the Secure by Design Government Standard, the Data Protection by Design Process and receive a review from the Data Privacy Team, the Data Protection Officer and final sign-off from the SIRO, or those with delegated rights. This is to ensure that the NHSBT follows its obligations as a Data Controller to ensure the security of the data we are responsible for and individuals are fully informed about how their data is being used and can exercise their rights should they object to the processing.

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

Data collection should be kept to a minimum and relevant to support the purpose for which it is needed. If additional data would support the service but is not necessary for the purpose (for example the collection of religious beliefs would support better donor engagement) this field can be added but it must be clear to the individual the data is not mandatory and they have a clear free choice whether or not to provide the data with no impact on the care or service, they receive.

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

Reasonable steps should be taken to validate the information provided and ensure it is kept up to date. This includes consistent and correct use of identifiers such as NHS number, or unique Donor number on all correspondence. Should an individual query the accuracy of the information this should be reviewed and where errors are found corrected without delay.

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

The Information Asset Owner is responsible for ensuring all assets have set retention periods in accordance with SPN189 Records Retention specification and the NHS Records Management Code of Practice 2021.

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

Correct organisational and technical measures to protect the data must always be in place, this should be identified and put in place before the data is collected from Individuals. Secure by Design and the Data Protection by Design process should be followed, and a Data Protection Impact Assessment (DPIA) must be completed and reviewed by Data Privacy Team and the DPO with final sign-off from the SIRO or those with delegated authority before the data is obtained.
Article 5(2) adds that:

"**The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."**

The principles lie at the heart of the UK GDPR. They are set out right at the start of the legislation and inform everything that follows. They don't give hard and fast rules but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the UK GPDR.

Failure to comply with the principles may leave NHSBT open to substantial fines. Article 83 of the General Data Protection Regulation provides details of the possible administrative fines that could be levied against NHSBT. There are two tiers of penalties fines, the higher maximum, and the standard maximum. The standard maximum penalty first is up to €10 £8.7 million or 2% of annual global turnover of the previous year, whichever is higher. The higher maximum penalty second is up to €20 £17.5 million or 4% of annual turnover of the previous year, whichever is higher. Breaches of controller or processor obligations will be fined within the first tier, and breaches of data subjects' rights and freedoms will result in the higher level fine. the higher maximum amount can apply to any failure to comply with any of the data protection principles, any rights an individual may have under Part 3 or in relation to any transfers of data to third countries. If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply.

**Individuals' Rights**

The UK GDPR imposes legal obligations on organisations under articles 12-23 of the UK GDPR to comply with 8 fundamental individual rights. Most of these rights are not absolute and a dependent on the identified lawful basis for processing, other regulatory or statutory obligations may supersede an individual's data rights. Any request from an individual either verbal or in writing to apply their rights must be processed within 1 month and can extend to 2 months if the request is complex, the Senior Records and Disclosure Manager, or the Data Protection Officeris ultimately responsible for advising whether a right should be applied.

Data Protection Impact Assessments is the organisations main risk asessment tool to ensure individual rights are not breached by implementing a new system or process or changes to existing systems or processes .

**1. The right to be informed.**

At the point of obtaining information form an individual NHSBT must explain the purposes for processing their personal data, retention periods, and who it will be shared with.

This data is held centrally in the NHSBT Privacy notice.

**2. The right of access**

Individuals have the right to access their personal data, this is commonly referred to as subject access request. **MPD11** must be followed.

**3. The right to rectification**

Any individual has the right to seek rectification of their records should the information contained within be incorrect. In most circumstances this right is absolute if it is agreed by both parties that the information is incorrect. Existing data should not be removed but records updated to show the change.

A clinical record should never be retrospectively amended, even if its is agreed by all parties to contain inaccurate data, instead a note of the correct information should be made clear.

**4. The right to erasure or right to be forgotten.**

This right is not absolute; many factors should be considered when reviewing an application from an individual to apply this right. When considering this right, it is important to understand the lawful basis being relied on for processing the data, if relying on consent the individual has a much stronger case.
NHSBT has regulatory and statutory obligations for tractability and clinical record keeping which must not be compromised when applying this right. In most circumstances it will be more appropriate to apply the right to restrict processing rather than full erasure.

For the blood service a Donor retains the right to be forgotten up to the point of the session screening process. Once a DHC is received and a clinical decision has been made whether or not the individual is eligible to be a donor, the right to be forgotten no longer applies. The right to restrict processing would then apply.
For the Organ Donor register or national transplant registry either a donor or recipient can invoke their right to be forgotten up until the point where they have received clinical care.

As a rule the right to be forgotten will be restricted where specified in Art 17 (3) as follows:

*a) for exercising the right of freedom of expression and information;*
*b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

*c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);*

*d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims*

**5. The right to restrict processing**

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time. Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data, but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

**6. The right to data portability**

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller. The right to data portability only applies when: our

lawful basis for processing this information is consent or for the performance of a contract; and the Organisation is carrying out the processing by automated means (ie excluding paper files).

**7. The right to object**

An individual can object to their data being processed where data is processed for scientific or historical research, or statistical purposes, the right to object is more restricted. When applying this right, the individual should explain their reasons for wanting to object to processing. The DPO will have to decide if the processing is in the public interest or if there are other regulatory or statutory obligations on NHSBT to retain and continue processing the data this will be decided on a case-by-case basis and will depend on clinical implications for both donor and recipient.

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

The UK GDPR gives an individual the right not to be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them. These provisions restrict when we can carry out this type of processing and give individuals specific rights in those cases.

Article 22(1) of the UK GDPR limits the circumstances in which we can make solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. We can only carry out this type of processing if we can rely on one of the three exceptions set out in Article 22(2). These exceptions are not the same as the lawful bases for processing required under Article 6.

Article 22(4) provides an additional layer of protection for special category personal data. We can only carry out the processing described in Article 22(1) if one of the above exceptions applies and:

- We have the individual's explicit consent; or
- the processing is necessary for reasons of substantial public interest. Substantial public interest conditions are set out in Schedule 1 Part 2 of the DPA 2018.

DUAA introduces Article 22A, which maintains a similar approach to automated decision-making to that currently set out in the UK GDPR above but clarifies that a decision is 'solely automated' only where there is no 'meaningful' human involvement. It is also mandatory to consider the extent to which any decisions have been reached in reliance on automated profiling when assessing whether there is meaningful human involvement. This higher threshold therefore places a renewed emphasis on demonstrable human oversight. When any Department at NHSBT is using Artificial Intelligence or algorithmic tools human oversight must be demonstrated. This will be particularly relevant when exploring AI assisted triage, eligibility assessments, or resource allocation.

NHSBT are required by law under our 2005 Directions to provide the organ offering schemes. There is substantial public interest as the use of algorithms in the offering

schemes is necessary for the purposes of equality of treatment for those requiring organs, with a view to enabling such equality to be promoted or maintained. As such, we rely on Article 9(2)(g) under Article 22 (4).

Any proposed or actual profiling or automated decision making that results in a legal or similarly significant effect on the data subject, requires a full Data Protection Impact Assessment.(DPIA)IA.

**Artificial Intelligence (AI) and Algorithmic Governance**

Any directorate procuring, piloting, developing, or deploying Artificial Intelligence (AI), machine learning models, or automated algorithmic decision-making tools must adhere to the following mandatory governance standards prior to live operational use:

1. **Mandatory Pre-Deployment DPIA Gate:** A comprehensive Data Protection Impact Assessment (DPIA) addressing AI-specific privacy, security, and ethical risks must be completed by the Information Asset Owner (IAO), evaluated by the Data Privacy Team, and formally signed off before personal data is ingested or processed.
2. **Controller Oversight & Vendor Safeguards:** NHSBT must maintain data controller (or joint controller) status when partnering with technology vendors. Third-party processing contracts must strictly prohibit external suppliers from using NHSBT donor, patient, or workforce data to train commercial models without explicit, documented legal authorization.
3. **Meaningful Human Oversight (UK GDPR Art. 22 & DUAA Art. 22A):** Solely automated decision-making that produces legal or similarly significant effects on individuals is prohibited unless expressly mandated by law. Where algorithmic tools assist clinical triage, donor eligibility, or staff rostering, systems must operate in an augmented advisory capacity with demonstrable, substantive human review and intervention.
4. **Transparency & Explainability:** Data subjects must be informed via public privacy notices and clinical communications where AI or automated processing is deployed. Clinicians and operational decision-makers must record algorithmic recommendations within the individual's record and be equipped to explain the underlying logic in plain language.
5. **Statistical Accuracy, Fairness & SaMD Compliance:** AI models must undergo rigorous pre-procurement validation to ensure clinical accuracy, consistency, and mitigation of algorithmic bias (supported by an Equality Impact Assessment). Where an AI application falls within the regulatory definition of Software as a Medical Device (SaMD), full MHRA certification and UKCA compliance must be verified prior to deployment.
6. **Data Minimisation & Security Architecture:** AI systems must process only the minimum personal data strictly necessary, prioritising de-identified, pseudonymised, or synthetic datasets for model validation. Systems must enforce multifactor authentication, strict role-based access controls, comprehensive audit logging, and data-loss prevention controls to prevent unauthorized export.

**Commented [AO8]:** Aligns with Cover Paper Section 2 & Operational Implications (Item 6: AI Governance Framework). Enforces pre-deployment DPIA gates, prohibits vendor training on NHSBT data, and mandates demonstrable human oversight under DUAA Art. 22A for clinical triage and workforce algorithms.

7. **Transparency, Explainability & Algorithmic Recording:** Data subjects must be informed where AI or automated processing is deployed, and clinicians or operators must be equipped to explain recommendations in plain language. Any algorithmic tool materially influencing decisions affecting individuals must comply with the UK Algorithmic Transparency Recording Standard (ATRS), with formal transparency records maintained prior to live operational use.

**Formatted:** Font: Not Bold

**Wearable Recording Technologies and Perimeter Privacy**

**Commented [AO9]:** Aligns with Cover Paper Section 2 & Operational Implications (Item 7: Wearable Technologies / Smart Glasses). Establishes site perimeter controls and reception signage across donation sessions, laboratories, and clinical areas following recent regulator guidance.

To safeguard the confidentiality and dignity of donors, patients, and staff:

1. **Perimeter Prohibition:** The use of wearable recording hardware, including smart glasses, hidden optical cameras, and wearable audiovisual recording devices to capture images, video, or audio of donors, patients, or staff across NHSBT premises, blood donation sessions, laboratories, and clinical facilities is strictly prohibited.
2. **Public Signage & Transparency:** Clear advisory notices and updated privacy notices must be maintained at session reception points and patient-facing facilities, establishing that recording devices must not be operated on site.
3. **Incident Enforcement:** Any unconsented recording or dissemination of donor, patient, or employee data on public or social media platforms will be treated as a security breach and managed under NHSBT's security, disciplinary, and safeguarding procedures.

**Formatted:** No bullets or numbering

**Definitions**
A glossary of terms and definitions routinely used in data protection is given as an appendix to this document

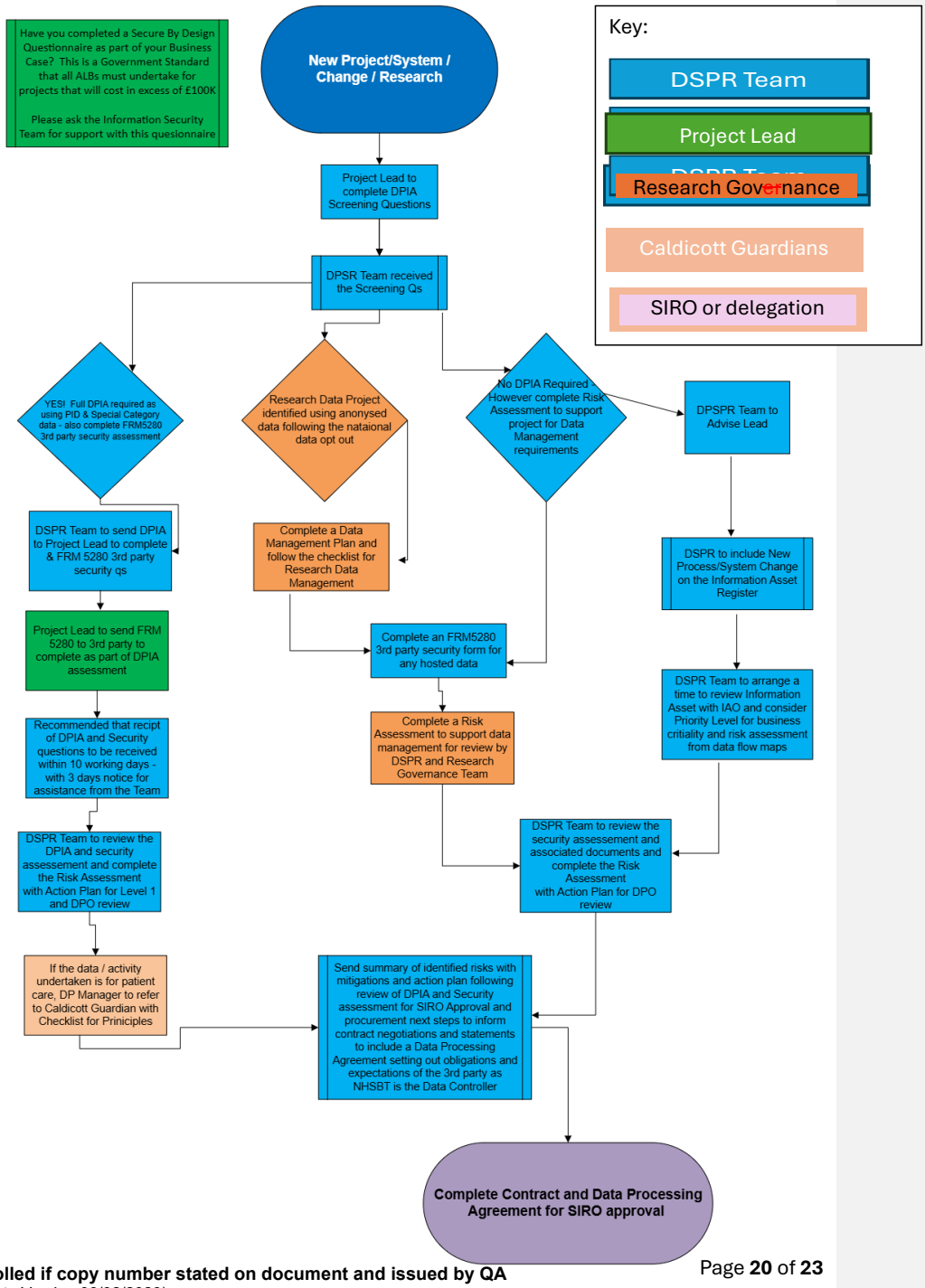
**Related Documents / References**

- POL266 - NHS Blood and Transplant Data Security, Privacy and Records Management Policy
- FRM5280 - Information Governance Risk Report and Procurement Methodology
- POL10 - NHSBT Information Security Policy
- MPD11 - Handling of Data Protection Subject Access Requests
- SPN189 - NHSBT Record Storage
- MPD1655 - Conducting a Data Protection Impact Assessments on Corestream
- POL209 - Data Security, Privacy and Records Management (DSPR) Awareness Training
- POL247 - Patient Registration for Transplantation
- NHSBT Code of Conduct
- NHSBT Disciplinary Policy and Procedure
- Confidentiality: NHS Code of Practice
- 'To Share or Not to Share?' The Information Governance Review (Caldicott 2)
- Appendix 5 for definition of personal data

**Appendices**

Appendix 1 - Flow Chart

Appendix 2 - Glossary of Terms


Have you completed a Secure By Design Questionnaire as part of your Business Case? This is a Government Standard that all ALBs must undertake for projects that will cost in excess of £100K
Please ask the Information Security Team for support with this quesionnaire
New Project/System / Change / Research
Project Lead to complete DPIA Screening Questions
DPSR Team received the Screening Qs
YES! Full DPIA required as using PID & Special Category data - also complete FRM5280 3rd party security assessment
Research Data Project identified using anonysed data following the nataional data opt out
No DPIA Required - However complete Risk Assessment to support project for Data Management requirements
DPSPR Team to Advise Lead
DSPR Team to send DPIA to Project Lead to complete & FRM 5280 3rd party security qs
Complete a Data Management Plan and follow the checklist for Research Data Management
DSPR to include New Process/System Change on the Information Asset Register
Project Lead to send FRM 5280 to 3rd party to complete as part of DPIA assessment
Complete an FRM5280 3rd party security form for any hosted data
DSPR Team to arrange a time to review Information Asset with IAO and consider Priority Level for business critiality and risk assessment from data flow maps
Recommended that recipt of DPIA and Security questions to be received within 10 working days - with 3 days notice for assistance from the Team
Complete a Risk Assessment to support data management for review by DSPR and Research Governance Team
DSPR Team to review the DPIA and security assessement and complete the Risk Assessment with Action Plan for Level 1 and DPO review
DSPR Team to review the security assessement and associated documents and complete the Risk Assessment with Action Plan for DPO review
If the data / activity undertaken is for patient care, DP Manager to refer to Caldicott Guardian with Checklist for Priniciples
Send summary of identified risks with mitigations and action plan following review of DPIA and Security assessment for SIRO Approval and procurement next steps to inform contract negotiations and statements to include a Data Processing Agreement setting out obligations and expectations of the 3rd party as NHSBT is the Data Controller
Complete Contract and Data Processing Agreement for SIRO approval
Key:
DSPR Team
Project Lead
Research Governance
Caldicott Guardians
SIRO or delegation

**Appendix 2**

**Glossary of Terms**

**UK GDPR -** The **General Data Protection Regulation** (EU) 2016/679

**Individual's –** Any living person whose data is being processed by NHSBT, this can include but is not limited to; Donors, Recipients, staff members, third party contractors.

~~**Information Commissioner's Office (ICO) –** The body that oversees the implementation of and compliance with the GDPR, Data Protection Act 2018, the Freedom of Information Act 2000 and the Environmental Information Regulations 2005). See www.ICO.org.uk.~~

Information Commission – The statutory body that oversees the implementation of and compliance with the GDPR, Data Protection Act 2018, the Freedom of Information Act 2000 and the Environmental Information Regulations 2005.

**Data Controller –** The legal body (in this case the NHSBT) which determines the purposes and manner of processing personal data and is legally responsible for the proper management of those personal data.

**Data Processor** – An individual or company which undertakes processing of personal data on behalf of a Data Controller.

**Personal Data** – Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. Personal data may exist in electronic or hard copy format, including databases, emails, paper files, audio tapes, CCTV tapes, etc.

**Processing –** Doing almost anything with personal data or set of personal data, including collecting, using, storing, viewing, analysing, disclosing, updating, amending, archiving or destroying it.

**Data Subjects** – The individuals that the information or data is about.

**Notification** – The system by which Data Controllers ~~inform the ICO of the purposes~~ inform the **Information Commission** of the purposes for which they process personal data. This information is published as a Register of Data Controllers and accessible online at www.ico.org.uk.

**Data Protection Principles –** The eight principles of good information handling which form the basis of the requirements of the Act

**Caldicott Principles**: The eight principles of handling and sharing patient/donor information across the NHS established by the committees chaired by Dame Fiona Caldicott

**Subject Access Request** – The process by which Data Subjects may request disclosure of their information held by a Data Controller.

**Third Party –** Anyone other than the Data Subject, the Data Controller and any Data Processor.

**Pseudonymisation and Anonymisation –** Pseudonymisation and Anonymisation are different in one key aspect. Anonymisation irreversibly destroys any way of identifying the data subject. Pseudonymisation substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject.

**Data Minimisation -** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed