Changes in this version

Enter changes here. Reference the step that the change is within. Put changes to instructions in purple.

Board Level Policy

1. Policy Purpose

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, the Access to Health Records Act 1990, the NHS Confidentiality Code of Practice, and the reports of the National Data Guardian

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

2. Scope of Application

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 NHSBT Chair, Executive and Non-Executive members of the NHSBT Board
- The NHSBT Executive
- Contracted third parties working under the direction of NHSBT
- Any individuals who have access to our data, including but not limited to temporary staff, consultants, and volunteers

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.

3. Policy statement and detail

In the course 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) and Data Protection Act 2018. 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.

Policy

NHSBT must respect and protect the privacy of all individuals, be they donors, patients, employees or other supporters, with whose information it 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. 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 properly incorporates 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 NDG's role is to help make sure the public can trust their confidential information is securely safeguarded and make sure that it is used to support citizens' care and to achieve better outcomes from health and care services.

The NGD is guided by four main principles objectives:

1. Safeguard trust in the confidentiality of our health and social care system
2. Encourage safe and appropriate information sharing for individual care.
3. Support understanding and engagement about how and why data is used.
4. Encourage the safe, appropriate, and ethical use of data in system planning, research and innovation that benefits the public.

Compliance with the NDG recommendations and reviews is mandated through the Data Security Protection Toolkit (DSPT). NHSBT's Information Governance Committee (IGC) is responsible for managing DSPT compliance.

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 UK 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 Data Protection Officer or 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.

Lawful Basis for Processing

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)

"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 Protection Officer or the DSPR Team

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 in Appendix 5 of 'To Share or Not to Share?' The Data Privacy Review (Caldicott 2). Care must be taken to assess the data items both singly and in combination, to establish the degree to which they may identify individuals.

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.

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.

Specific Requirements of the UK General Data Protection Regulations

Information and guidance about the UK GDPR are available from the Information Commissioner's website at ICO.org.uk. Article 5 of the UK 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 Data Protection by Design Process and receive sign off from Data Privacy and the Data Protection Officer. This is to ensure 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 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. The Data Protection by Design process should be followed, and a Data Protection Impact Assessment (DPIA) must be completed and approved by Data Privacy and the DPO 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 Data Protection Officer is ultimately responsible for advising whether a right should be applied.

Data Protection Impact Assessments are the organisations main tool to ensure individual rights are not breached by new process changes.

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 Handling of Data Protection Subject Access Requests 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*

SOP5552 outlines the process to complete a registrant's request to exercise their Right to be Forgotten.

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

This right only applies when processing data under explicit consent, it allows the data subject to move their data from one digital platform to another. This right will only apply in NHSBT in very limited circumstances.

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 depending on the impact on the individual.

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.

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, including via an algorithm, must undergo a DPIA.

NHSBT is required to report our use of algorithmic tools to the Algorithmic Transparency Recording Standard (ATRS). The ATRS is a framework for capturing information about algorithmic tools, including AI systems. It is designed to help public sector bodies openly publish information about the algorithmic tools they use in decision-making processes that affect members of the public.

4. Roles and responsibilities

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, in POL266 NHSBT's overarching Data Security, Privacy and Records Management policy, and related documents.

Under this policy, the Data Protection Officer (DPO) will be responsible for:

- Ensuring the policy is fit for purpose going forward, including ensuring it meets the requirements and controls for compliance by NHSBT.
- Ensuring the policy is reviewed regularly and specifically on change of regulation or as a result of learnings from any notifiable incidents.
- Ensuring breaches are properly managed and reported in a timely way to ICO as appropriate.
- Deciding on requests for rights-to-object (or other such requests by subjects on NHSBT) in order to reach an organisational position.

The SIRO will support and challenge the DPO in relation to the fulfilment, purpose and performance of this policy.

The Senior Data Security & Privacy Manger is responsible for maintaining NHSBT's notification to the Information Commissioner's Office (ICO), as required under the Data Protection Act 2018. The Information Governance Committee (IGC), formal sub-committee of the Audit, Risk and Governance Committee (ARGC) is responsible for review of this policy, responsibility for approval of this policy rests with the NHSBT Board.

5. Training and awareness

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

6. Reporting in relation to policy

Reporting in relation to confidentiality and data protection involve a structured process whereby data protection incidents are reported as outlined in MPD828. Key Performance Indicators (KPIs) are regularly reported to the Information Governance Committee (IGC). This includes a detailed analysis of any incidents, ensuring that all relevant data is thoroughly examined and understood. The Compliance Dashboard is escalated to the Audit and Risk Governance Committee (ARGC), providing a comprehensive overview of performance and any potential risks. This hierarchical reporting structure ensures that critical information is communicated effectively and that appropriate actions can be taken at each level of governance.

7. Related policies and procedures

- POL266 - NHS Blood and Transplant Data Security, Privacy and Records Management Policy
- MPD828 - Information Risk Incident Management
- 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

8. Policy Review and Compliance Monitoring

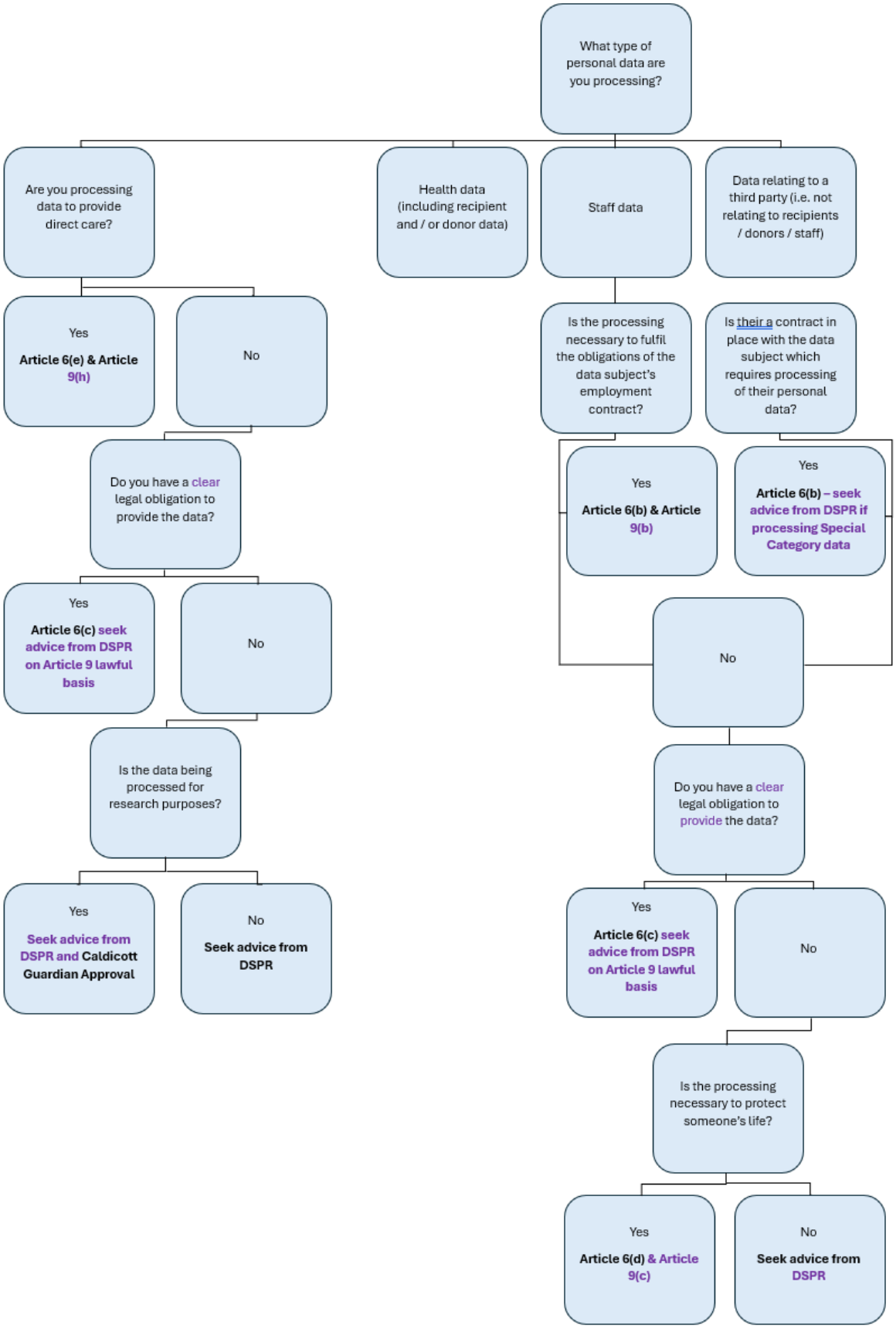
Element/Activity being monitored	Lead/roles	Reporting arrangements and frequency	Recommendations/actions
Policy review	Head of DSPR & DPO	Audit, Risk and Governance Committee Annually	The policy will be reviewed subject to new or amended pertinent legislation / guidance publish and / or evolution in best practice
Assurance on Compliance	Head of DSPR & DPO	Information Governance Committee Bi-monthly	Review of data privacy and security incidents and subject access request compliance rates.
Policy/process effectiveness	Head of DSPR & DPO	Audit, Risk and Governance Committee Annually	Annual report on effectiveness of policy / processes
Breaches	Head of DSPR & DPO	Notifiable breaches - Audit, Risk and Governance Committee All other breaches – Information Governance Committee As and when they arise	Notifiable breaches – DPO, Caldicott Guardian and SIRO notification, and Information Commissioner's Office notification. Appropriate action to be taken as appropriate.

9. Version Control and RACI view

Version	Owner	Approved by and basis of changes	Approved Date	Effective Date	Date of Next Review
1.0	Chief Digital and Information Officer	ARGC subject to comments prior to Board approval Board	07/03/2025 01/04/2025	Tbc	Within a year of last approval

(R) Responsible	Head of Data Security, Privacy and Records and Data Protection Officer
(A) Accountable	Chief Digital and Information Officer
(C) Consultees	ARGC
(I) Informed	All staff

Appendix 1


What type of personal data are you processing?
Are you processing data to provide direct care?
Health data (including recipient and / or donor data)
Staff data
Data relating to a third party (i.e. not relating to recipients / donors / staff)
Yes
Article 6(e) & Article 9(h)
No
Do you have a clear legal obligation to provide the data?
Yes
Article 6(c) seek advice from DSPR on Article 9 lawful basis
No
Is the data being processed for research purposes?
Yes
Seek advice from DSPR and Caldicott Guardian Approval
No
Seek advice from DSPR
Is the processing necessary to fulfil the obligations of the data subject's employment contract?
Is their a contract in place with the data subject which requires processing of their personal data?
Yes
Article 6(b) & Article 9(b)
Yes
Article 6(b) – seek advice from DSPR if processing Special Category data
No
Do you have a clear legal obligation to provide the data?
Yes
Article 6(c) seek advice from DSPR on Article 9 lawful basis
No
Is the processing necessary to protect someone's life?
Yes
Article 6(d) & Article 9(c)
No
Seek advice from DSPR