

Title:	Policy on the Data Protection and Protection of Personal Information		
Policy Author(s)	[REDACTED] Senior Manager Data Protection Tel: [REDACTED]@belfasttrust.hscni.net		
Responsible Director:	Alastair Campbell, Performance, Planning and Informatics Director		
Policy Type: (tick as appropriate)	*Directorate Specific ☐	Clinical Trust Wide ☐	Non Clinical Trust Wide ☒
If policy type is confirmed as *Directorate Specific please list the name and date of the local Committee/Group that policy was approved			
Approval process:	Policy and External Guidance Assurance Committee Executive Team		Approval date: 06/02/2024 26/02/2024
Operational Date:	February 2024		Review Date: February 2029
Version No.	6	Supersedes	V5 – May 2018 – May 2023
Key Words:	Privacy, data protection, information governance, UK GDPR		
Links to other policies	Legislation - UK General Data Protection Regulation 2018 UK Data Protection Act 2023 Trust Policies - <u>BHSCT ICT Security Policy (2018) TP 72/11</u> <u>BHSCT/PPI (02) (221) Records Retention and Disposal Schedule</u> <u>BHSCT Records Management Policy (2018) TP 13/08</u> <u>BHSCT Policy for Processing requests for access to Patient and Client Records (2018) TP 60/10</u> <u>BHSCT Data Access for Organisations External to the Trust (20148) TP 69/10</u> <u>BHSCT Social Media Policy (2019) TP 76/11</u> <u>BHSCT Transportation of Records Policy (20184) TP 85/13</u> <u>BHSCT Policy for Reporting & Managing Adverse Incidents (2020) TP 08/08</u> Guidance - DoH Code of Practice on protecting the confidentiality of service user information (April 2019)		

1.0 INTRODUCTION / SUMMARY OF POLICY

1.1 Background

Through its day to day operations the Belfast Health And Social Care Trust is required to collect and hold certain types of personal data including information about people with whom it deals with in order to operate.

The legal requirement for the Trust and its staff to treat personal information confidentially and hold it securely is set out in the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018. The introduction of GDPR in 2018 brought EU countries into line with previously unforeseen ways that data is now used. The legislation introduced tougher fines for non-compliance and breaches, and gives individuals more say over what can be done with their data. This legislation places the concept of confidentiality within a legal framework and imposes both corporate and individual responsibilities.

1.2 Purpose

The lawful and correct handling of personal data by the staff of Belfast Health & Social Care Trust is crucial to the success and maintenance of confidence between the Trust and those with whom it deals, both internally and externally.

The legislation makes provision for the regulation of the processing of personal information relating to **living** individuals, including the obtaining, holding, use, disclosure and destruction of such information.

This policy has been introduced with the aim of empowering managers to be proactive in relation to the protection of personal information in their workplace.

This Policy should be read in conjunction with following policies:-

- BHSCT Records Management Policy
- BHSCT ICT Security Policy
- BHSCT Data Sharing Policy
- BHSCT Social Media Policy
- BHSCT Transportation of Records Policy
- BHSCT Guidelines for Processing requests for access to Patient/Client and Personal Records.
- BHSCT Records Retention & Disposal Policy
- BHSCT Adverse Incident Reporting and Managing Policy

1.3 Objectives

The Belfast Health & Social Care Trust needs to collect and use certain types of information about people with whom it deals in order to operate. These

include current, past and prospective employees, suppliers, clients, service users, patients and others with whom it communicates.

In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments or other bodies (e.g. Police Service of Northern Ireland). This personal information must be dealt with properly regardless of how it is collected, recorded and used – whether on paper, in a computer or recorded on other material – there are safeguards to ensure this in the UK GDPR and the Data Protection Act 2018.

The lawful and correct treatment of personal information by Belfast Health & Social Care Trust is regarded as very important to the success of our operation and to maintaining confidence with those the Trust deals with. To this end, the Trust fully endorses and will adhere to the principles of data protection as enumerated in the UK GDPR (see Appendix 1). The recently revised Caldicott principles (Appendix 2) also provide very practical standards in relation to handling personal information. It should be noted that the duty to share information can be as important as the duty to protect patient confidentiality.

2.0 SCOPE OF THE POLICY

This policy will apply to all staff. It is vital that this and the supporting policy and procedures are implemented and adhered to by all existing and new staff, including for examples: students, trainees, individuals on placement and volunteers. This also includes those contracted temporarily, such as GPs and locums, and anyone reviewing records for the purpose of audit e.g. RQIA.

The UK GDPR covers all personal information handled within the Trust relating to **living** individuals, including that held on paper, electronic, digital, archival and back up media and being processed for any purpose i.e research, audit, provision of care etc. This also includes all personal information that is appropriately removed/transferred/viewed by staff [REDACTED]

It should be noted that the Freedom of Information Act 2000 is a separate piece of legislation which gives the public a right of access to types of 'recorded' information held by Public Authorities; it does not in general apply to personal information.

3.0 ROLES AND RESPONSIBILITIES

Trust Responsibilities

The Trust and any organisation or persons carrying out functions on its behalf, have a legal obligation to safeguard personal information and a duty to support staff exercising ethical standards of confidentiality. In order to fulfil these responsibilities, the Trust will ensure that this policy is disseminated to

all staff, that it is understood and adhered to. Organisations carrying out functions on behalf of the Trust should also provide the Trust with assurances that they and their staff comply fully with the UK GDPR.

The Trust Chief Executive has nominated joint responsibility for the role of Personal Data Guardian to the Medical Director and the Executive Director of Social Work. The Personal Data Guardian actively supports work to facilitate and enable information sharing and advises on options for lawful and ethical processing of information as required.

The Information Governance Board chaired by the Director of Performance, Planning and Informatics has responsibility for monitoring compliance and effectiveness of information and personal data security within the Trust.

The Chief Executive's and Directors Responsibilities

Ultimately, responsibility for all aspects of processing personal information lies with the Chief Executive. However, responsibility is delegated to individual Directors within each service group for personal information within that area. Therefore, Directors have specific responsibilities to:

- Satisfy themselves that this policy and associated policies and procedures are implemented for their area of responsibility;
- Ensure personal information is used only for purposes for which it was obtained.

The Senior Information Risk Owners (SIRO) Responsibilities

The SIRO as a Director of the Trust is familiar with information risks and is the focus for the management of information risk at Board level. The Director of Performance, Planning and Informatics is responsible for this within the Trust and therefore has a key role in ensuring that the Trust complies with its legal responsibilities in this regard.

The Information Asset Owner (IAO) Responsibilities

The role of an IAO is to understand what information is held, what is added and what is removed, how information is moved and who has access and why. As a result they have a key role to understand and address risks to information and to lead and foster a culture that values, protects and uses information for the public good.

They are responsible for maintaining and updating the Information Asset Register (IAR) [REDACTED]

[REDACTED]. They are responsible for ensuring that they attend training appropriate for the role when offered by the Trust and ensure that all staff in their directorate complete Mandatory Data Protection training [REDACTED]. This role is undertaken by a number of Co-Directors within the Belfast Trust, with an additional reporting function to the SIRO. [REDACTED]

Managers' Responsibilities

Managers have specific responsibilities in the implementation of this policy and in monitoring compliance with it. This includes:

- The implementation of the general procedures within their departments;
- The preparation and implementation of specific departmental procedures, where necessary and appropriate;
- Ensuring that all staff receive mandatory training [REDACTED] in the protection of personal information; and are familiar with the content of this policy.
- Monitoring adherence to procedures on a day-to-day basis and reporting any data breaches to the Information Governance Department and relevant IAO in a timely manner. For serious data breaches, this needs to be done as soon as possible to ensure that reporting to the Information Commissioner's Office is carried out within 72 hours.

Individual Members of Staff Responsibilities:

All Trust staff

have a responsibility to abide by the principles contained within this document and adhere to the associated procedural guidelines. These documents are complementary to the ethical duty of confidence contained within the professional regulations for health and social care professionals. Staff should be aware that failure to adhere to the guidance given in this policy and related procedures could result in them being personally liable under the UK GDPR and may also result in disciplinary action and could lead to criminal proceedings by the PSNI or action from the ICO. All staff working or training in the Trust should ensure that they receive initial data protection training and update training

4.0 CONSULTATION

Information Governance and Records Management Group

5.0 POLICY STATEMENT/IMPLEMENTATION

Key Policy Principles

Definitions - See Appendix 2 for key definitions within the legislation.

5.1 Key Policy Statement

Every citizen needs to feel confident that information about their Health & Social Care is securely safeguarded and shared appropriately when that is in their interest. Everyone working in the Trust should see information governance as part of their responsibility.

The aim of this policy is to empower managers to be pro-active in relation to the processing of personal information in their workplace. It is vital that the policy and supporting procedures are implemented and adhered to by all existing and new staff [REDACTED]

[REDACTED] and anyone reviewing records for the purpose of audit or investigations [REDACTED]

All users of personal data within the Trust have a responsibility to ensure that they process the data in accordance with the seven data protection principles taken from the UK GDPR summarised in Appendix 1. As part of the legislation the Trust shall be responsible for, and be able to demonstrate, compliance with the principles. There is significantly more accountability required with the UK GDPR legislation.

5.2 Policy Principles

Obtaining Personal Information

- Personal information should not be collected or used unless there is justification, both legally and practically, for doing so. A clear purpose should be documented where possible.
- Individuals should be told how their personal information might be used before they are asked to provide it.
- The Trust should provide guidance on how personal information is being processed i.e. through Privacy Notices. As well as overarching privacy notices, individual services may also wish to ensure patients/clients are aware of how their information will be processed in local leaflets and guidance.
- Personal Identifiable data collected for the Health or Social care of the service user may not be used for any other purpose e.g. research without an appropriate lawful basis. All staff should contact their Information Governance (IG) department for further advice before using information for a secondary purpose.
- Where a particular use of information is not essential, the explicit consent of individuals to the use of their personal information will be sought, in advance of their being asked to provide it. There should be a legal basis for the processing of all information within the Trust.

In cases of consent for vulnerable adults and children please see Department of health guidance - [Code of Practice on Protecting the Confidentiality of Service User Information](#) | [Department of Health \(health-ni.gov.uk\)](#).

In line with statutory obligations the service should determine if each patient has capacity to understand and retain information relating to providing consent. The process of seeking consent needs to be a meaningful one, in that refusal has to be understood as an option. In addition, means of effective

communication needs assessed and reasonable adjustments provided to support accessibility; the healthcare professional should utilise the NI Health and Social Care Interpreting Service Procedure for Booking Interpreters, rather than using family or carers.

Data Protection Impact Assessment

- A DPIA forms part of the 'privacy by design' approach to the handling of personal information and allows services to demonstrate compliance with data protection legislation. It is **mandatory for services to complete a DPIA** when introducing any new system or service that will involve the processing of personal data. A DPIA can be used to identify and reduce the privacy risks of projects and can reduce the risks of harm to individuals through the misuse of their personal information. It is important to begin completion of the DPIA at the outset of the process to avoid delays at a later stage.
- A DPIA is needed when:
 - Introducing new software, system or database
 - Making significant changes to an existing system or process
 - Introducing a new way of gathering information (online as opposed to paper)
 - Making a change to the way information is stored or secured
- Guidance on the completion of the DPIA and the DPIA template can be found on the Information Governance page on the Loop.

Records and Record Keeping

- Personal information should be adequate, relevant and not excessive for the reason(s) for which it is collected or used.
- Personal information should be accurate and kept up to date.
- All records should be clear, relevant and concise and indicate the identity of any persons who have made an entry in them. The use of abbreviations and jargon should be avoided unless they are from agreed lists.

See **Records Management Policy** for further guidance.

Security of Personal Information

- Appropriate measures must be taken against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. See **ICT Security Policy** for further information.
- Services should take reasonable steps to ensure that they have adequate and secure facilities for the storage of personal information and that access is restricted to only those who need it.

- To avoid unauthorised disclosure care must be taken to site PC's and terminals so that they are not visible to unauthorised people. Care must be taken to ensure that manual records, files and printouts etc. are not left where they can be accessed by unauthorised staff.

Access to Personal Information

Requests for access to personal information should be dealt with in line with current Trust procedures, whether made by the individual, their representative, or person with parental responsibility and in keeping with the requirements of the UK GDPR. Before releasing a copy of any personal data you must check with the Medical Legal department for acute records or the Data Protection Office for community records, mental health, social care and staff records.

- Requests by the PSNI and solicitors should be discussed with the Data Protection and Medical Legal teams before disclosure
- Original records should never be released to anyone (including the PSNI) unless directed by a court.
- Staff should be aware that accessing personal identifiable information without an appropriate lawful basis could be deemed as a criminal offence under section 170 of the Data Protection Act 2018 or if the information was accessed using a computer system, could be deemed an offence under section 1 of the Computer Misuse Act 1990
- Staff should only access data that is relevant for their area of work, Trust systems are audited to identify usage. Staff should never use their access to Trust systems in order to access their own records or those of family/friends or anyone not connected to their role in work; the Subject Access Request (SAR) process is the appropriate route to obtain this information. Inappropriate access to personal data can result in disciplinary action, potentially defined as gross misconduct, specifically, but not restricted to, breaches of confidentiality. The Trust must report these breaches to the ICO who will undertake a separate investigation which could lead to prosecution.

See Guidelines for Processing Requests for Access to Patient/Client and Personal Records, for further information.

Sharing Personal Information

- Access to personal information should be controlled and information released on a 'need to know' basis and in compliance with the legislation or other legitimate expressed instruction. Unless there is an essential purpose or legal requirement only anonymised and/or aggregated information should be released.
- Any personal information given or received in confidence for one purpose may not be used for a different purpose, or passed to anyone else without

the knowledge and consent of the individual concerned (or, if appropriate their representative).

- The disclosure of personal information should be restricted to only as much information as is necessary for the purpose.
- In cases where a bulk transfer of person-identifiable information is to be shared with an external body for secondary purposes i.e. not direct patient care, it will be necessary to complete the Trust's Data Access Agreement (DAA) form. Personal data is where an individual can be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the data controller i.e. the Trust.
- A DAA ensures appropriate procedures have been adhered to and that there is authorisation for the sharing of data. See **Policy on the Access to Data for Organisations External to the Trust**.
- The wishes of an individual to withhold or restrict the transfer of his/her personal information should be respected. However, this does not override the Trust's responsibility, in designated circumstances, to provide information for legal or statutory purposes or to protect the public.
- Any sharing of personal identifiable data should be redacted in line with redaction guidance when necessary and shared securely [REDACTED]
[REDACTED]
Redaction guidance is available [REDACTED]
- Staff should never email identifiable data to their personal email accounts and should never disclose the email address of personal accounts to other recipients of an email. Blind carbon copy (bcc) should be used when sending emails to more than one personal account

Movement and Transport of Personal Information

- Paper-based files containing personal information will only be removed from storage areas when necessary and their location should be tracked at all times.
- All staff are responsible for the movement of records around the Trust [REDACTED]
[REDACTED]
[REDACTED]

Personal information will be transferred by secured means and only to places where the Trust is satisfied that it will receive an adequate level of protection. See **Transportation of Records Policy** and **ICT Security Policy**.

Retention and Destruction of Personal Information

- Personal information will not be kept for longer than is necessary for the reason(s) for which it was collected.

- Records containing personal information will be destroyed on a timely basis and in line with the Trust's **Policy on the Retention and Disposal of Records**.
- Once identified as appropriate for destruction, personal information will be disposed of in such a manner that it is not possible to reconstitute the data.
- Confidential waste should be used for the routine disposal of personal identifiable data.
- [REDACTED]
- Staff involved in the management of the records should regularly attend Archive Training to ensure that they are adequately trained in the process of archiving records.

Use of Technology

- Technology will be used in such a way as to assist the protection of data [REDACTED]
- The Trust will encourage new ways of working with the Information Communication Technology (ICT) Department to maximise the secure access, storage and transfer of data.
- Staff are not permitted to use Social Media sites or messaging apps to share personal identifiable information. [REDACTED]
- [REDACTED]
- The use of digital apps endorsed by the Trust are subject to UK GDPR and all personal information should be processed in line with this policy and associated policies.

- [REDACTED]

- Staff working remotely must comply with all Trust policies and procedures and take additional steps to ensure the security and confidentiality of personal data. [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Further guidance is available in the **Records Management policy**, the **ICT Security policy**, **Social Media policy** and the **Transportation of Records Policy**.

Data Breaches

- The legislation now requires organisations to report data breaches which meet the criteria to the ICO within 72 hours of becoming 'aware' of a breach. Failure to do so may result in the Information Commissioners Office (ICO) taking further action.
- All data breaches must be reported **verbally** and in writing to the Information Governance department as soon as the department becomes aware of the breach or potential breach. Any data breach must be recorded [REDACTED]. All data breaches must be investigated thoroughly and appropriate action taken.

Training and Communication

- Staff should understand their responsibilities with respect to the proper handling of data through attendance at either:-
 - induction [REDACTED]
 - mandatory data protection training sessions [REDACTED] or
 - by completing the e-learning module [REDACTED]

A range of training courses are made available [REDACTED]

Cyber Security

The Trust is vulnerable to cyber security threats. Both the NHS in England and the HSE in the Republic of Ireland have had catastrophic cyber-attacks. It is important that the Trust take all necessary steps to protect its network. Therefore, if you are:

- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
- Using another organisation or 3rd party [REDACTED]
[REDACTED]
[REDACTED]. Either a Contract, Data Sharing Agreement (DSA), Memorandum of Understanding (MOU) or Service Level Agreement (SLA) should be in place to cover the data protection requirements.

CCTV

- CCTV is primarily in place for the protection of service users and staff and for the detection or prevention of crime. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- Access to CCTV should be tightly controlled [REDACTED]
[REDACTED].
- There should be adequate signage where CCTV is in use to alert staff and service users and an appropriate privacy notice in place, which outlines its uses.
- [REDACTED]
[REDACTED]

For more information, please see Trust guidance documents on CCTV.

Development of Policies & Procedures

A range of policies have been developed by the Information Governance Board and its subgroups to assist with complying with Data Protection legislation. Further policies will be developed as necessary.

5.3 Dissemination

This policy will be circulated to all Directors and IAO's for dissemination.

5.4 Resources

This policy will be available on The Loop and communicated to staff during Information Governance training sessions and incorporated in the Information

Governance Bulletins. A staff booklet entitled 'Employee's Guide to Handling Information' is available to all new staff as a precursor to training, or from the Information Governance Team for existing staff.

[REDACTED]

[REDACTED] Adequate auditing and deletion capabilities must be built into the specification of all new information systems, in accordance with the UK General Data Protection Regulation 2018.

5.5 Exceptions

There are no exceptions.

6.0 MONITORING AND REVIEW

It is the responsibility of line managers to monitor the completion and review of staff training and information governance incident reporting and investigation. Other specific monitoring responsibilities will be under the remit of the Information Governance Board.

7.0 EVIDENCE BASE / REFERENCES

UK General Data Protection Regulation
Data Protection Act 2018
"Code of Practice on Protecting the Confidentiality of Service User Information" issued by DHSSPS – revised April 2019
Information Commissioners Office website - www.ico.gov.uk

8.0 APPENDICES

Appendix 1 Seven Principles of the Data Protection Act.
Appendix 2 Eight Caldicott Principles

9.0 NURSING AND MIDWIFERY STUDENTS

Nursing and/or Midwifery students on pre-registration education programmes, approved under relevant 2018/2019 NMC education standards, must be given the opportunity to have experience of and become proficient in the **Policy on the Data Protection Act 2018 and Protection of Personal Information** where required by the student's programme. This experience must be under the appropriate supervision of a registered nurse, registered midwife or registered health and social care professional who is adequately experienced

in this skill and who will be accountable for determining the required level of direct or indirect supervision and responsible for signing/countersigning documentation.

Direct and indirect supervision

- Direct supervision means that the supervising registered nurse, registered midwife or registered health and social care professional is actually present and works alongside the student when they are undertaking a delegated role or activity.
- Indirect supervision occurs when the registered nurse, registered midwife or registered health and social care professional does not directly observe the student undertaking a delegated role or activity. (NIPEC, 2020)

This policy has been developed in accordance with the above statement.

Wording within this section must not be removed.

10.0 **EQUALITY IMPACT ASSESSMENT**

The Trust has legal responsibilities in terms of equality (Section 75 of the Northern Ireland Act 1998), disability discrimination and human rights to undertake a screening exercise to ascertain if the policy has potential impact and if it must be subject to a full impact assessment. The process is the responsibility of the Policy Author. The template to be complete by the Policy Author and guidance are available on the Trust Intranet or via this [link](#).

All policies (apart from those regionally adopted) must complete the template and submit with a copy of the policy to the Equality & Planning Team via the generic email address Equality@belfasttrust.hscni.net

The outcome of the equality screening for the policy is:

Major impact	☐
Minor impact	☐
No impact	☐

Wording within this section must not be removed

11.0 **DATA PROTECTION IMPACT ASSESSMENT**

New activities involving collecting and using personal data can result in privacy risks. In line with requirements of the General Data Protection Regulation and the Data Protection Act 2018 the Trust considers the impact on the privacy of individuals and ways to mitigate against any risks. A screening exercise must be carried out by the Policy Author to ascertain if the policy must be subject to a full assessment. Guidance is available on the Trust Intranet or via this [link](#).

If a full impact assessment is required, the Policy Author must carry out the process. They can contact colleagues in the Information Governance Department for advice on Tel: [REDACTED]

Completed Data Protection Impact Assessment forms must be returned to the Equality & Planning Team via the generic email address [REDACTED]@belfasttrust.hscni.net

The outcome of the Data Protection Impact Assessment screening for the policy is:

Not necessary – no personal data involved ☐
A full data protection impact assessment is required ☐
A full data protection impact assessment is not required ☐

Wording within this section must not be removed.

12.0 RURAL NEEDS IMPACT ASSESSMENT

The Trust has a legal responsibility to have due regard to rural needs when developing, adopting, implementing or revising policies, and when designing and delivering public services. A screening exercise should be carried out by the Policy Author to ascertain if the policy must be subject to a full assessment. Guidance is available on the Trust Intranet or via this [link](#).

If a full assessment is required the Policy Author must complete the shortened rural needs assessment template on the Trust Intranet. Each Directorate has a Rural Needs Champion who can provide support/assistance.

Completed Rural Impact Assessment forms must be returned to the Equality & Planning Team via the generic email address [REDACTED]@belfasttrust.hscni.net

Wording within this section must not be removed.

13.0 REASONABLE ADJUSTMENT ASSESSMENT

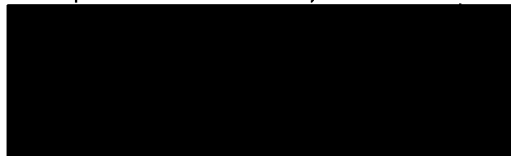
Under the Disability Discrimination Act 1995 (as amended) (DDA), all staff/ service providers have a duty to make Reasonable Adjustments to any barrier a person with a disability faces when accessing or using goods, facilities and services, in order to remove or reduce such barriers. E.g. physical access, communicating with people who have a disability, producing information such as leaflets or letters in accessible alternative formats. E.g. easy read, braille, or audio or being flexible regarding appointments. This is a non-delegable duty.

The policy has been developed in accordance with the Trust's legal duty to consider the need to make reasonable adjustments under the DDA.

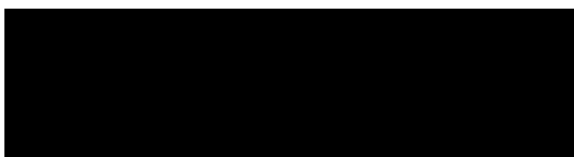
Wording within this section must not be removed.

SIGNATORIES

(Policy – Guidance should be signed off by the author of the policy and the identified responsible director).



Date: 06/02/2024



Date: 03/03/2024

Name Alastair Campbell

Title Director Performance, Planning and Informatics

Appendix 1 Seven Principles of the Data Protection Act.

The UK GDPR principles require that personal information:

Article 5 of the UK GDPR requires that;

1 Personal data shall be;

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

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;

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

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;

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; and

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.”

2. The Controller shall be responsible for and be able to demonstrate compliance with, paragraph 1

Revised Caldicott Principles

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their Responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. 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.

8. Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required

Appendix 2 Definitions

Eight Caldicott Principles

Terms	Definition
UK GDPR	The UK General Data Protection Regulation (UK GDPR) The UK General Data Protection Regulation (GDPR) sets out key principles, rights and obligations when processing personal data. It sits alongside the Data Protection Act 2018 (DPA) and incorporates the EU GDPR.
UK Data Protection Act 2018	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
Data Controller	A controller determines the purposes and means of processing personal data.
Data Processor	A processor is responsible for processing personal data on behalf of a controller.
Personal Data	The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
Special Categories of Personal Data	The UK GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).
Data Protection Impact Assessments	Data Protection Impact Assessments (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.