Wirral Community Health and Care NHS Foundation Trust

Data Protection and Confidentiality Policy
IG10
Version 1.1

TRUST-WIDE NON-CLINICAL

Document detail	
Policy Number	IG10
Version	Version 1.1
Approved by	Quality and Safety Committee
Effective from	November 2021
Date of last review	11/2018
Date of next review	10/2024
Lead Director	Executive Medical Director / Caldicott Guardian
Responsible Lead	Information Governance Manager / Data Protection Officer
Superseded documents	IG04 Caldicott and Data Protection Policy, IG01 Information Governance and Data Protection Policy, IG07 Confidentiality Code of Conduct Policy
Document summary	The policy provides a robust framework to ensure a consistent approach to both compliance and best practice for data protection and confidentiality across the whole organisation, and supports the duties set out in the NHS Constitution and the requirements of the NHS Confidentiality Code of Practice 2003.

Document History		
Version number	Comments	Approved by
1	This policy has been updated to ensure that it provides a clear statement of organisational intent in relation to data protection and confidentiality. This has led to the policy being separated into an Information Governance and Data Protection Policy.	Quality and Safety Committee
1.1	Supersedes Confidentiality Code of Conduct Policy and removed reference to the document – minor changes	Information Governance and Data Security Group

SUPPORTING STATEMENTS

This document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Wirral Community Health & Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child/adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/adult concern';
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role; ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Wirral Community Health & Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session.

EQUALITY AND HUMAN RIGHTS

Wirral Community Health & Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the protected characteristics of age, disability, gender, reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation. The Equality Act also requires public authorities to have due regard to the need to eliminate unlawful discrimination against someone because of their marriage or civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Wirral Community Health & Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Wirral Community Health & Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity and **A**utonomy

Policy on a Page

This policy provides a robust framework to ensure a consistent approach to both compliance and best practice for data protection and confidentiality across the whole organisation, and supports the duties set out in the NHS Constitution and the requirements of the NHS Confidentiality Code of Practice 2003.

The Trust will at all times comply with the Data Protection Principles set out in Article 5 of the UK GDPR. These principles specify (in summary) that Personal Data must be:

- processed fairly and lawfully and transparently (Principle1)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Principle 2)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle 3)
- accurate and up to date (Principle 4)
- kept no longer than necessary (Principle 5)
- protected in appropriate ways from unauthorised use, loss or disclosure (Principle 6)

Data subjects will be given straightforward procedures to enable them to exercise their rights set out below. Subject access procedures are available on the Trust website. The Trust will seek to comply with the statutory time limits for subject access requests. The Trust will comply with the Information Commissioner's Subject Access guidance.

The Trust will ensure that data protection is considered at the start of any new project, service, or process. A DPIA identifies and assesses potential risks to the Trust of processing activities. It is an integral part of data protection by design and by default, and the Trust will ensure DPIAs are completed for all projects, proposals or business changes that involve personal information.

The Trust and its staff shall at all times comply with the law of confidentiality, the requirements of the GDPR and DPA and the Human Rights Act 1998 so far as they affect confidentiality obligations and with the eight Caldicott principles (National Data Guardian, 2020) which specify that the Trust should:

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

The Trust and its staff shall follow the five confidentiality rules set out by HSCIC Guide to Confidentiality 2013:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

CONTENTS **Page No.**

1. PURPOSE AND RATIONALE

This policy provides the framework to ensure that the Trust complies with the requirements of statutory and legal frameworks relating to the use of Personal Confidential Data, including:

- Data Protection Act 2018
- UK General Data Protection Regulation
- Health & Social Care (Quality & Safety) Act 2015
- Common Law Duty of Confidentiality
- The Privacy and Electronic Communications Regulations 2003
- Health & Social Care Act 2012
- National Health Service Act 1977, 2006
- Freedom of Information Act 2000
- Public Records Act 1958, 1967 and 2005
- Network & Information Systems Regulations 2018
- Information: To Share Or Not To Share? The Information Governance Review (National Data Guardian, 2003)
- The Eight Caldicott Principles (National Data Guardian, 2020)
- Confidentiality: NHS Code of Practice (Department of Health and Social Care, 2003)
- Records Management Code of Practice 2021 (NHSX, 2021)
- Data Security & Protection Toolkit
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs (National Data Guardian, 2016)
- Care Quality Commission Standards
- Environmental Information Regulations 2004
- Human Rights Act 1998
- Access to Health Records Act 1990
- Serious Crime Act 2015
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998

The policy provides a robust framework to ensure a consistent approach to both compliance and best practice for data protection and confidentiality across the whole organisation, and supports the duties set out in the NHS Constitution and the requirements of the NHS Confidentiality Code of Practice 2003.

The Trust is registered as a data controller that is processing personal information with the Information Commissioner's Office. The Trust's registration number is Z2567487.

Although the UK GDPR does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as to one who is alive. There is also separate legislation that applies when accessing health records of a deceased person, the Access to Health Records Act 1990. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought in the first instance from the Data Protection Officer wcnt.DPO@nhs.net

Staff should be aware that failure to comply with this policy, associated policies and procedures and/or their data protection responsibilities is serious and could result in a number of sanctions including:

- Disciplinary action up to and including dismissal
- Criminal charges
- Investigation and potential removal of registration by relevant Professional Body i.e. Nursing and Midwifery Council

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

The objectives of the Data Protection and Confidentiality Policy are to establish:

- the Trusts position on Data Protection regulations
- a robust framework to ensure a consistent approach to both compliance and best practice for data protection and confidentiality across the whole organisation
- key actions with assigned responsibilities
- a requirement for all staff appointed by the Trust to adhere to the policy

3. SCOPE

This policy applies to all:

- employees of the Trust, including Non-Executive Directors, Governors, bank staff, volunteers, individuals on secondment, trainees, those on a training placement as well as locum or temporary staff employed through an agency
- non-Trust employees who process personal data using information systems provided for them to perform their role within the organisation or who handle documentation on behalf of the Trust
- contractors and third parties appointed by the Trust to process personal data on behalf of the Trust
- areas of Trust business, for example, HR, clinical divisions, finance, estates
- personal and special category data created and received
- formats of information for example, clinical/care records, emails, voice messages, minutes, photographs, staff records, financial records and facilities records
- information systems and applications
- equipment used to process personal confidential data information for example, laptops, computers, mobile phones, cameras

4. DEFINITIONS

Term	Definition
UK GDPR	Is the retained version of the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales
DPA	Sets out Data Protection framework for UK and replaces Data Protection Act 1998
Data	For the purposes of this policy data includes recorded information in any form or format, whether hard copy or electronic, and whether part of a formal information system or simply held transiently.
Data Subject	Someone who can be identified as a person, or with a combination of other information can be identified
Data Processor	An entity that processes data for and on behalf of the Trust
Data Controller	An entity that decides how and why personal data is used i.e. the Trust
Processing	Any operation or set of operations which is performed on Personal Data
Pseudonymisation	The processing of personal data in a way that it cannot be attributed to a specific data subject without the use of additional information, provided that additional information is kept

	separate
Personal Data	Any information, which directly or indirectly can identify an individual such as name, identification number or contact details
Special Category Data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

5. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

Chief Executive Officer
As the accountable officer the Chief Executive Officer is responsible for overall leadership and management of the Trust and has the ultimate responsibility for ensuring compliance with the Data Protection Act 2018, UK GDPR, Human Rights Act 1998, and the common law duty of confidentiality.

Trust Board
The Board will review Data Protection and Confidentiality concerns escalated from the Information Governance and Data Security Group via the Quality and Safety Committee and Finance and Performance Committee. Additionally, Trust Board will receive reports at least annually on the Trust's Information Governance performance.

Senior Information Risk Owner
The Director of Corporate Affairs is the Trust's Senior Information Risk Owner (SIRO.) SIRO has Executive responsibility for management and mitigation of all information risk.

The SIRO will:

- review and agree action in respect of identified information risks
- brief the Board on identified information risk issues
- ensure that all information assets have assigned information asset owners
- annually sign off the information asset register
- ensure that the organisations approach to information risk is effective in terms of resource, commitment and execution and that it is communicated to staff
- take ownership of the risk assessment processes for information and cyber risk
- oversee the development and implementation of an incident risk policy (NHS Digital, 2018)

The SIRO is a core member of the Information Governance and Data Security Group and reports directly to the Chief Executive Officer.

Caldicott Guardian
The Executive Medical Director is the Caldicott Guardian of the Trust and has a strategic role with regard to representing and championing data protection and confidentiality at Board and where appropriate, throughout the Trust.

The Caldicott Guardian will:

- ensure that personal information collected about patients / service users is used legally, ethically and appropriately, and that confidentiality is maintained
- apply the eight Caldicott Principles wisely, using common sense and an understanding of the law

- actively support work to enable information sharing where it is appropriate to share and advising on options for lawful and ethical processing
  (UK Caldicott Guardian Office, 2017)

The Caldicott Guardian is a core member of the Information Governance and Data Security Group and reports directly to the Chief Executive Officer.

Quality and Safety Committee
The Quality and Safety Committee (QSC) is the responsible committee for the final approval of this policy.

The QSC will:

- receive assurance that the Trust meets its statutory and regulatory obligations in relation to Data Protection and Confidentiality via the Information Governance and Data Security Group
- review concerns escalated to them, action those relevant to the Committee's terms of reference and refer, as appropriate, to the Board
- encourage and review incident reporting within the Trust

Information Governance and Data Security Group
The Trust's Information Governance and Data Security Group is responsible for reviewing and approving this policy prior to ratification by QSC.

The Information Governance and Data Security Group will:

- oversee and support Trust compliance with the Data Security and Protection Toolkit (DSPT) and consequently measure performance against the National Data Guardian's ten data security standards
- ensure compliance with legislative and regulatory requirements of information governance
- receive Cyber Security Assurance through monthly IT Security Group report
- review information governance and data security guidance relevant to the Trust and escalate them when appropriate to QSC
- monitor information assets and data flows captured within the Information Asset Register
- monitor Information Governance / Record Keeping incidents and trends, system access audits outcomes and SAFE IG checklist compliance
- monitor mitigations, controls and progress of Information Governance and Data Security risks and escalate them to QSC in line with the Policy for Risk Identification and
- review and monitor Freedom of Information, Environmental Information Regulation and Subject Access Requests
- monitor, review and approve information governance and data security policies, procedures and guidance in a timely way to support compliance with legislative and regulatory requirements prior to endorsement by QSC
- identify organisations with which personal data is routinely and regularly shared and develop suitable information sharing arrangements
- review and approve requests for the destruction of records in line with Records Management Code of Practice 2021
- review and approve Data Protection Impact Assessments produced as part of a privacy by design approach to new projects and ways of processing
- oversee action plans that are developed as a result of information governance and data security incidents, Situation, Background, Assessment and Recommendation (SBAR) or from complex Root Cause Analysis (RCA) investigations and escalate them to the appropriate group or committee
- monitor outcomes of annual record keeping and information quality audits and identify learning

- monitor incidents and trends of inappropriate access to confidential information
- monitor staff compliance with e-Learning for healthcare Data Security Awareness Level 1 and specialist staff compliance with training identified from annual Training Needs Analysis

Information Governance Manager
The Information Governance Manager is the author of this policy.

The Information Governance Manager will:

- manage and oversee the Trusts information governance agenda
- provide information governance and data protection advice and guidance to staff
- monitor compliance with information governance policies and procedures and ensure policies are in line with legislator and regulatory requirements
- maintain an awareness of information governance and data protection issues within the Trust
- submit an annual Information Governance Report (including compliance with Data Protection requirements) to the Board
- complete SBAR and RCA investigations as and when required and subsequently support the development of actions plans
- report data security and protection risks on the risk register and to the SIRO
- ensure compliance with and annually submit the DSPT
- support the teams that handle Subject Access Requests and Freedom of Information requests
- assess data security and protection incidents and when required onward report to Information Commissioner's Office (ICO) and/or Department of Health
- provide support and advice to Information Asset Owners in relation to their assets
- develop and deliver bespoke information governance and data protection training
- be a core member of the Information Governance and Data Security Group
- provide support and work closely with the SIRO and Caldicott Guardian on information governance and data protection issues

Data Protection Officer
As required by Article 37 of UK GDPR the DPO will:

- monitor organisational compliance with data protection legislation
- inform and advise the Trust and its employees on data protection obligations
- review Data Protection Impact Assessments (DPIAs)
- cooperate with the ICO
- be the first point of contact for the ICO and individuals whose data is processed by the Trust (patients, service users, staff, volunteers etc.)
  (NHS Digital 2018)

Divisional/Locality Managers and Service Leads
Divisional/Locality Managers and Service Leads will:

- ensure the Data Protection and Confidentiality Policy is implemented within their divisions/localities and ensure service level procedures are compliant with the Data Protection Policy
- monitor staff compliance with e-Learning for healthcare Data Security Awareness Level 1
- encourage staff to report any data security and protection incidents via the incident reporting system immediately
- report any identified information risks relating to their divisions/services on the Trust's risk register
- To ensure that the development of any new processes or systems will be compliant with Data Protection and Confidentiality requirements

All Staff
This policy applies to all employees of the Trust, including Non-Executive Directors, Governors, bank staff, volunteers, individuals on secondment and trainees or those on a training placement within the Trust as well as locum or temporary staff employed through an agency.

Staff will:

- ensure that they are aware of Data Protection and Confidentiality requirements and standards including responsibilities in relation to their specific role and are compliant with these standards and responsibilities
- complete annual information governance training (e-Learning for Healthcare Data Security Awareness Level 1) via the Electronic Staff Record (ESR)
- report identified data security and protection incidents on the Trusts incident reporting system

6. DATA PROTECTION

6.1 Data Protection Principles

The Trust will at all times comply with the Data Protection Principles set out in Article 5 of the UK GDPR. These principles specify (in summary) that Personal Data must be:

- processed fairly and lawfully and transparently (Principle1)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Principle 2)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle 3)
- accurate and up to date (Principle 4)
- kept no longer than necessary (Principle 5)
- protected in appropriate ways from unauthorised use, loss or disclosure (Principle 6)

6.2 Compliance – Principle 1 ('lawfulness, fairness and transparency')

The Trust will put in place procedures and measures to ensure compliance with Principle 1 including but not limited to:

- Maintaining Privacy Notices (available on the Trust public website for patients/service users and Staff Zone for staff) for all types of data processed which are kept up to date, made available to data subjects, and comply with the requirements of the UK GDPR and any Code of Practice issued by the Information Commissioner's Office (ICO)
- Appointing a Data Protection Officer, whose contact details are available to data subjects
- Complying with the Common Law Duty of Confidentiality
- Ensuring that the lawful basis for the processing of information is identified and included in Privacy Notices
- Ensuring that, where processing is by consent, such consent is freely given, specific, informed and unambiguous and obtained via a statement or by a clear affirmative action and in the case of Special Category Data such consent is explicit
- Informing individuals of data breaches that may result in a risk to their rights and

freedoms
- Ensuring that Personal Data is not informally shared with or disclosed to any third party. Any such sharing or disclosure will be controlled and appropriately authorised, will only be done where it is lawful to do so and notified to data subjects (if consent has not been obtained) unless UK GDPR or DPA provide an exemption and there is good and lawful reason to apply that exemption. When sharing Personal Data the Trust will comply with any Code of Practice issued by the ICO.

For patients the Trust identifies that in most cases Personal Data is processed in exercise of its official authority under various statutory duties including the requirement to maintain securely an accurate, complete and contemporaneous record in respect of each service user under Regulation 17 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (Article 6(1)(e) UK GDPR). In so far as patient records comprise Special Category Data the legal basis is typically that processing is necessary for the purposes of preventive or occupational medicine, or the provision of health or social care or treatment or the management of health or social care systems (Article 9(2)(h) UK GDPR).

6.3 Compliance – Principle 2 ('purpose limitation')

The Trust will put in place procedures and measures to ensure compliance with principle 2 including but not limited to:

- Maintenance of an Information Asset Register (IAR). The IAR will record the lawful basis for processing of the assets and the controls over any related data flows including information sharing and processing arrangements
- Completion of Data Protection Impact Assessments for high risk processing.

6.4 Compliance – Principle 3 ('data minimisation')

The Trust will put in place procedures and measures to ensure compliance with principle 3 including but not limited to:

- Conducting routine audits as part of good data management practice
- Ensuring that relevant records policies and professional guidelines are adhered to including appropriate Clinical Record keeping standards
- Ensuring that all processing of Personal Data is kept to the minimum necessary for compliance with the Trust's work and purposes and access to any Personal Data is restricted to those who need it for their work
- Ensuring that, where possible without interfering with the Trust's necessary work, or that of any third party with whom data is shared or to whom data is disclosed, any Personal Data is anonymised or pseudonymised before being used, shared or disclosed. The Trust will comply with the Information Commissioner's Anonymisation Code of Practice and NHS Guidance
- Maintaining registers of data sharing and data processing agreements with third parties. Data processing agreements will conform to the requirements of Articles 28 to 32 GDPR, be in writing, and impose equivalent responsibilities on any data processor to those set out in this policy

6.5 Compliance – Principle 4 ('accuracy')

The Trust will put in place procedures and measures to ensure compliance with principle 4 including but not limited to:

- Ensuring that data users record information accurately and take reasonable steps to check the accuracy of information they receive from data subjects or anyone else
- Conducting routine audits as part of good data quality management practice

- Providing guidance to staff on good records management practices including guidance on Clinical Record keeping standards
- Advising data subjects of their right to seek rectification and ensuring requests are acted upon as required
- Auditing annually information quality and records management against standards set out in both the Records Management Policy

6.6 Compliance – Principle 5 ('storage limitation')

The Trust will put in place procedures and measures to ensure compliance with principle 5 including but not limited to:

- Maintaining and regularly reviewing a Records Management Policy or policies and procedures covering the creation, management and secure disposal of corporate, staff and patient records
- Ensuring that services regularly review what information is held and what information has met the end of its retention
- Compliance with the Records Management Code of Practice 2021 (NHSX, 2021)
- Ensuring secure and appropriate disposition of information that reaches the end of its retention

6.7 Compliance – Principle 6 ('integrity and confidentiality')

The Trust will put in place procedures and measures to ensure compliance with principle 6 including but not limited to:

- Ensuring an appropriate level of protection and security to personal data
- Maintaining and regularly reviewing an IT Security Policy and associated procedures
- Maintaining and regularly reviewing a Policy and associated procedures for investigating and managing breaches or suspected breaches of data protection, confidentiality and/ or information security
- Completion of Data Protection Impact Assessments (DPIA) for new and changing high risk processes which handle Personal Data
- Ensuring that data protection by design and by default is built into its processes, in particular in relation to commissioning new information assets, new methods of processing and the use of new technology
- Complying with NHS and Government Security Management Standards including cyber security
- Ensuring that all Information Assets are owned and managed and risk assessments of those assets and associated information flows are undertaken and reviewed at appropriate intervals
- Maintaining a program of data protection, security and confidentiality audits
- Ensuring that appropriate guidance and training is available to staff on the steps they must take to comply with this policy
- Complying with the National Data Guardian's (NDG) Data Security Standards and completing annually the NHS Data Security and Protection Toolkit as evidence of compliance
- Granting staff appropriate and role relevant levels of access to personal data
- Ensuring that any transfer of Personal Data outside of the European Union is compliant with Articles 44-49 of GDPR. Such transfers will not be made without consultation with the Trust's Data Protection Officer and in the case of confidential patient data without the approval of the Trust's Caldicott Guardian. Approvals and consultation may relate to regular or individual transfers
- Ensuring services have developed Business Continuity Plans in line with the Emergency Planning, Resilience and Response Policy

- Monitoring and investigating all reported instances of actual or potential breaches of confidentiality and security.

7. INDIVIDUAL RIGHTS

Data subjects will be given straightforward procedures to enable them to exercise their rights set out below. Subject access procedures are available on the Trust website. The Trust will seek to comply with the statutory time limits for subject access requests. The Trust will comply with the Information Commissioner's Subject Access guidance.

The Trust will where appropriate take into account the Information Commissioners Office (ICO) guidance on Access to Information in Complaints Files, and in relation to subject access requests by employees the ICO Employment Practices Code and Supplementary Guidance.

The Trust will maintain appropriate procedures and guidance for both staff and those interacting with the Trust to ensure that individuals are given and can exercise their rights under UK GDPR including:

- The right to information about the processing of their Personal Data under Articles 13 and 14 of GDPR in the form of privacy notices on the Trust website and in contracts, information leaflets, and explanations in correspondence where appropriate;
- The right of access to their Personal Data under Article 15 of GDPR;
- The rights of rectification, erasure and to restrict processing under Articles 16-18 of GDPR;
- The right to object to processing under Article 21 GDPR and to limit automated individual decision making and profiling under Article 22.

8. DATA PROTECTION BY DESIGN AND DEFAULT

As part of the UK GDPR's accountability principle the Trust will safeguard individual rights by putting in place the appropriate technical and organisational measures. The UK GDPR requires the Trust to integrate data protection into every aspect of processing activity.

This includes implementation of the data protection principles and safeguarding individual rights, such as data minimisation, pseudonymisation and purpose limitation as set in this policy.

The Trust will ensure that data protection is considered at the start of any new project, service, or process.

9. DATA PROTECTION IMPACT ASSESSMENT

A DPIA identifies and assesses potential risks to the Trust of processing activities. It is an integral part of data protection by design and by default, and the Trust will ensure DPIAs are completed for all projects, proposals or business changes that involve personal information.

A template DPIA can be obtained on Staff Zone.

A list of approved DPIAs will be made available on the Trust's public website.

10. DATA SHARING – THIRD PARTIES

Where the Trust, as Data Controller, instructs a third-party organisation to process data on their behalf the Trust will ensure the processor provides "sufficient guarantees" that they have

the appropriate technical and organisational measures in place to ensure the processing complies with the UK GDPR and protects the rights of individuals.

11. CONFIDENTIALITY

11.1 Caldicott Principles

The Trust and its staff shall at all times comply with the law of confidentiality, the requirements of the GDPR and DPA and the Human Rights Act 1998 so far as they affect confidentiality obligations and with the eight Caldicott principles (National Data Guardian, 2020) which specify that the Trust should:

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

The Trust's appointed Caldicott Guardian (Executive Medical Director) will advise the Trust Board on matters of patient confidentiality and promote the safe and secure handling of patient data.

The Trust's Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures. The Caldicott Guardian can be contacted via email wcnt.caldicottguardian@nhs.net

11.2 Duty of Confidentiality

A duty of confidentiality is when one person discloses information to another e.g. patient to clinician in circumstances where it is reasonable to expect that information will be held in confidence. It is:

- A legal obligation derived from case law
- A requirement established within professional codes of conduct
- Included in all NHS staff members' contracts of employment.

It is essential that the Trust provides a confidential service. Breaches of that confidentiality may lead to regulatory investigation and can result in disciplinary measures to those who have been negligent in causing the breach (see section 11.5).

11.3 Patient/Service User Confidentiality

In March 2013, the Health & Social Care Information Centre published "A guide to confidentiality in health and social care" which identified five rules for handling Personal

Confidential Data about patients which encompass the Caldicott Principles. The Trust adopts and expects all staff to abide by those Rules:

Rule 1: Confidential information about service users or patients should be treated confidentially and respectfully.

- All staff are required to keep confidential any information regarding patients, service users and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner.

- Confidential information must not be disclosed to third parties without prior discussion and confirmation with a senior manager in the Trust.

- Staff should not access patient or staff information on any system (electronic or paper) that relates to family (including spouses; children; parents etc.) or friends, even if it is considered to be within their role in the organisation.

- Confidentiality clauses will be included in contracts of employment and engagement. Confidentiality clause will be included in contracts with 3rd party contractors and suppliers who process Personal Confidential Data.

Rule 2: Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

- The Trust and its staff will share information likely to facilitate the provision of health services or adult social care in the individual's best interests as required by S251B of the Health and Social Care Act 2015 providing this does not breach patient confidentiality.

- Sharing arrangements will be notified to patients through the Trust's Privacy Notice and will be routinely discussed with patients at point of contact whenever possible and appropriate. Where this is done consent to share may be implied for the purposes of direct care.

- Sharing within care pathways should be restricted to what is relevant necessary and proportionate.

- Sharing Personal Confidential Data without consent may be possible without breaching confidentiality as set out in Section 11.4.

Rule 3: Information that is shared for the benefit of the community should be anonymised

- Anonymised information may be shared for the benefit of the community including research and the management of health services. The Trust will apply the HSCIC Anonymisation Standard and have regard to any Code of Practice Issued by the ICO.

- Patient Personal Confidential Data which has not been anonymised or de-identified will not be used for purposes other than direct care unless:
  - the Trust has fully informed explicit consent
  - there is a legal obligation to do so – see section 11.4
  - the law allows sharing for a particular reason where there is overriding public interest e.g. control of infectious diseases or where regulations and legislation allow under s251 of the NHS Act 2006 – see section 11.4

Rule 4: An individual's right to object to the sharing of confidential information about them should be respected

- Where a patient objects to a disclosure, they should receive an explanation of the likely consequences of their decision but if it is maintained the objection must be respected except in exceptional circumstances - see section 11.4 for examples. An explanation should be provided to the individual.

- When considering an objection the Trust will take into account:
    - whether not supporting the objection will damage the effectiveness of care;
    - whether there is a demonstrable risk that the safety of the patient will be reduced by not upholding the objection; and
    - whether there are compelling legitimate grounds relating to the individual's situation

Rule 5: Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

- This policy and associated documents and procedures (see Section 12) are in compliance with Rule 5.

- Staff must report via Datix any incident or suspected incident in which security or confidentiality has or may have been breached in accordance with the Trust's Incident Management Policy.

- The local induction checklist requires managers to inform staff about the importance of information governance, information governance training requirements and to provide copies of the Information Governance Policy and Data Protection and Confidentiality Policy.

- Staff should not access any information relating to themselves, in Trust records, including Health and Employee records.

- The Trust will ensure that all organisations it shares confidential information with are committed to following the rules of confidentiality

11.4 Disclosing Information against an individual's wishes

In certain circumstances personal information may need to be disclosed without consent or even despite objections. In such cases staff must make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from their Team Leader/Senior Clinician or the Caldicott Guardian or Information Governance Manager.

Circumstances where the subject's right to confidentiality may be overridden are rare.

Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and

consultation.

Where appropriate the Trust's Safeguarding Policies must be followed.

In making decisions on disclosure without consent for non-care purposes the Trust will have due regard to the National Data Opt-Out. The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning.Patients can find out more about the wider use of confidential personal information and register their choice to opt out by visiting www.nhs.uk/your-nhs-data-matters

See Data Protection by Design and Default Procedure for further information.

The following are examples where disclosure is required by law and no consent is required:

- Births and deaths - National Health Service Act 1977
- Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
- Poisonings and serious accidents at the work place - Health & Safety at Work • Act 1974
- Terminations - Abortion Regulations 1991
- Child abuse - Children's Act 1989 and The Protection of Children Act 1999. Section 47 of the Children Act 1989 imposes a legal obligation to supply information to a Local Authority exercising its child protection powers unless it would be unreasonable to do so.
- Section 45 of the Care Act 2014 imposes a legal obligation to disclose to a Safeguarding Adults Board if certain conditions are met.
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998
- Section 8 of the National Audit Act 1983 imposes a legal obligation on public bodies to provide relevant information to the National Audit Office.
- S5B Female Genital Mutilation Act 2003
- Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes where it is not possible to use anonymised information and where seeking consent is not practical, having regard to the cost and technology available. S251 Approvals will be subject to the National Data Opt-Out in most cases.

11.5 Breach of data protection and confidentiality

Any breach or suspected breach of data protection and confidentiality can have severe implications for the Trust, our patients, and staff. Where significant numbers of patients are involved, this can impact on the reputation of the NHS as a whole.

The Trust will report serious breaches within 72 hours of the being made aware of the breach (where possible). The DPO is the single point of contact for all breaches and advice and guidance must be sought as soon as possible by contacting wcnt.dpo@nhs.net

Staff reporting incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Incident Management Policy.

Breaches of confidentiality or unauthorised disclosure of any information subject to the DPA and UK GDPR constitutes a serious disciplinary offence. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

12. RELATED POLICIES

This policy underpins the following policies/procedures:

Policy Name
The Information Governance Policy
Individual Rights and Accessing Records
Records Management Policy
Freedom of Information Policy
Data Protection by Default and Design Procedure
Data Protection Impact Assessment Policy
Information Security Policy
Policy for Risk Identification and Management
Emergency Planning, Resilience and Response Policy
Incident Management Policy
Duty of Candour Policy
Email Policy
Safe Use of Mobile Phones at Work Policy
Social Media SOP
Media SOP

13. TRAINING

It is compulsory for all new starters to complete onboarding prior to commencement in their post. Onboarding provides new employees with a data protection and security induction.

Managers must complete a local induction checklist with new starters. The local induction checklist requires managers to inform staff about the importance of information governance, information governance training requirements and to provide copies of the Information Governance Policy and Data Protection and Confidentiality Policy. Compliance with onboarding and the local induction checklist will be monitored through Education and Workforce Committee.

Staff are required to complete the Trust's information governance training annually (e-Learning for Healthcare Data Security Awareness Level 1) through ESR. The training period is 1st April – 31st March each year.

Information governance training is mandatory for all staff that have access to Trust information.

Managers with management responsibility for staff will be responsible for monitoring staff compliance with e-Learning for healthcare Data Security Awareness Level 1 and for ensuring that staff have sufficient time to complete training.

Bespoke information governance / data protection training will be provided by the Information Governance Manager on request by managers that have identified a training need within their team.

Staff with specialist roles are required to complete additional data security and protection training suitable to their role. Additional training requirements will be identified through the annual Training Needs Analysis.

Compliance with mandatory annual information governance training and training for staff with specialist roles will be monitored by the Information Governance and Data Security Group.

14. CONSULTATION

This policy has been reviewed by the Information Governance and Data Security Group prior to submission to the QSC.

15. DISTRIBUTION

The Information Governance Policy will be made available to all staff via Staff Zone. Staff will be informed of the release of this policy through the Staff Bulletin.

16. MONITORING

Key aspects of this policy will be monitored on a monthly basis by the Information Governance and Data Security Group:

Element to be monitored	Tool
Staff Training	% of staff that have completed Data Security Awareness E Learning with training period
Compliance with Data Protection and Confidentiality Policy	Number of data breaches reported to the Information Commissioners Office Number of incidents reported relating to Data Protection and Confidentiality
Individual Rights	Number of SARs responded to in statutory time scale
Data Protection by Design and Default	Number of Data Protection Impact Assessments completed

17. EQUALITY IMPACT ASSESSMENT

See Equality Impact Assessment in Appendix A.

18. REFERENCES

Department of Health and Social Care. (2003) *Confidentiality: NHS Code of Practice*. Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

Department of Health and Social Care. (2014) *Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.* Available from https://www.legislation.gov.uk/ukdsi/2014/9780111117613/introduction

Health and Social Care Information Centre. (2013). *A guide to confidentiality in Health and Social Care*. Available from https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care

Information Commisioner's Office. (2020). *Access to Information Held in Complaint Files.* Available from https://ico.org.uk/media/fororganisations/documents/1179/access_to_information_held_in_complaint_files.pdf

Information Governance Alliance. (2016) *Records Management Code of Practice for Health and Social Care.* Available from https://digital.nhs.uk/data-and-information/looking-after-

information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

National Data Guardian. (2016) *National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs*. Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

National Data Guardian. (2013) *Information: To Share Or Not To Share? The Information Governance Review.* Available from https://www.gov.uk/government/publications/the-information-governance-review

NHS Digital. (2018) *Data Security and Protection Toolkit Key Roles and the DPO*. Available from: https://www.dsptoolkit.nhs.uk/Help/2

UK Caldicott Guardian Council. (2017) A *Manual for Caldicott Guardians.* Available from https://www.ukcgc.uk/manual/contents

National Data Guardian. (2020) *The Eight Caldicott Principles.* Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf

Appendix A: Equality Impact Assessment

To be completed at the end of the policy. Write up prior to being submitted for approval.
If you are unsure and would like advice, please contact the Equality & Diversity Manager – wcnt.inclusion@nhs.net

Title	Data Protection and Confidentiality Policy Version 1
What is being considered?	The policy provides a robust framework to ensure a consistent approach to both compliance and best practice for data protection and confidentiality across the whole organisation, and supports the duties set out in the NHS Constitution and the requirements of the NHS Confidentiality Code of Practice 2003.
Who may be affected?	Patients [x] Staff [x] Public [x] Partner agencies [x]

Is there potential for an adverse impact against the protected groups below? Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual Orientation or the Human Rights articles?	Yes [ ] No [x]

On what basis was this decision made? (Please complete for both 'yes' and 'no').
All Trust employees, non-Trust employees who process personal data using systems provided and contractors and third parties appointed by the Trust to process personal data on behalf of the Trust must adhere to the framework set out in this policy to ensure compliance with Data Protection legislation and expected Confidentiality standards.
For example, you may wish to consider or refer to the some of the following:

- National Guideline / Report (DH / NICE / NSPA / HSE / other)
- Engagement feedback
- Previous Equality Impact screening
- Trust Committee / Multi Agency meeting

If 'No' equality relevance, sign off document below and submit this page when submitting your policy document for approval. If 'Yes' Please complete pages 2-3.
With regard to the general duty of the Equality Act 2010, the above function is deemed to have no equality relevance.

Equality relevance decision by Anna Simpson Title / Committee Quality and Safety Committee Date 12/10/2021