Caldicott and Data Protection Policy (N-027)

Version Number:	9.02
Author (name & job title)	Karen Robinson - Information Governance Officer
Executive Lead (name & job title):	Hilary Gledhill - Executive Director of Nursing, Allied Health and Social Care Professionals and Caldicott Guardian
Name of approving body:	BeDigital Group
Date full policy approved:	July 2018 (v9.00)
Date Ratified at Trust Board:	July 2018 (v9.00)
Next Full Review date:	March 2027

Minor amendments made prior to full review date above (see appended document control sheet for details)	
Date approved by Lead Director:	*Hilary Gledhill – 19 March 2024*
Date EMT as approving body notified for information:	*March 2024*

Policies should be accessed via the Trust intranet to ensure the current version is used

Contents

1. Introduction

Personal information held by the Trust is an important and valuable asset. The Trust recognises that the lawful and correct treatment of personal data is very important in delivering an effective health service and maintaining confidence with our patients.

Sharing personal information between service areas and partner agencies is vital for the provision of co-ordinated and seamless care of individuals. Legislation does not prevent the sharing of information but places important rules and safeguards that must be observed.

The aim of this policy is to describe the roles, responsibilities and principles for ensuring that personal information is handled in a lawful and correct manner.

2. Scope

This policy applies to all employees of the Trust, including all staff who are seconded to the Trust, contract, voluntary, temporary and agency staff and other people working on Trust premises. This includes members of staff with an honorary contract or paid an honorarium.

This policy applies to all personal data processed by the Trust as a data controller or a data processor.

3. Policy Statement

The Trust fully endorses the data protection principles set out in the UK General Data Protection Regulation and the Data Protection Act 2018. The Trust and all staff who process personal information must ensure these principles are followed. In summary these state that personal data shall be:

- processed lawfully, fairly and transparently
- collected for specified, explicit purposes (purpose limitation)
- adequate, relevant and limited to what is necessary (data minimisation)
- accurate and, where necessary, kept up to date.(accuracy)
- kept in an identifiable form for no longer than is necessary (storage limitation)
- processed in a manner that ensures appropriate security (integrity and confidentiality).

The Trust must be able to demonstrate compliance with the principles (accountability). The Trust does this by:

- adopting and implementing data protection policies;
- taking a ‘data protection by design and default’ approach and carrying out data protection impact assessments for changes in the use of personal data;
- ensuring written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of personal data processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- appointment of a data protection officer; and
- compliance with the Data Security and Protection Toolkit.

Furthermore, the Trust is committed to implementing the eight Caldicott principles for handling patient-identifiable information, namely:

- Justify the purpose of using patient identifiable information.
- Only use patient identifiable information when absolutely necessary.
- Use the minimum necessary patient identifiable information.

- Access patient identifiable information on a strict need to know basis.
- Everyone should be aware of their responsibilities.
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.
- Inform patients and service users about how their confidential information is used.

Any breach of the data protection legislation with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with Trust policy will be viewed as gross misconduct and may result in serious disciplinary action being taken, up to and including dismissal. Employees could also face criminal proceedings.

4. Definitions

Personal data	Any information relating to an identifiable natural person (data subject), identified either directly or indirectly by: Name, identification number, location data, online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	This term covers the collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment or combination, restriction, erasure or destruction of personal data.
Data Controller	The organisation that determines the purposes and means of processing personal data.
Data processor	The organisation that processes personal data on behalf of the controller.
UK GDPR	UK General Data Protection Regulation.
Special Category data	Sensitive personal data including racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, sexual orientation.

5. Duties and Responsibilities

5.1. Chief Executive

The Chief Executive has overall responsibility for Data Protection within the Trust.

5.2. Senior Information Risk Owner

The Senior Information Risk Owner will:

- Chair the Information Governance Group.
- Represent confidentiality and security issues at Trust Board level.
- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately briefed on information risk issues.

5.3. Caldicott Guardian

The Caldicott Guardian will:

- Act as the 'conscience' of the Trust regarding confidentiality, and ensure that the Trust satisfies the highest practical standards for the handling of patient information, both within the Trust and data flows to other NHS and non-NHS organisations
- Ensure that there is a framework enabling Caldicott principles to be reflected in Trust's policies and procedures for the management and use of personal information.
- Be a member of the Information Governance Group and participate in line with the terms of reference for that group.
- Fulfil the responsibilities as stipulated in this policy and the Information Governance Policy.
- Supports the Information Governance team (Head of Legal Services and Information Governance and IG Officers in the development of information sharing protocols.
- Offer support and advice as required to the Information Governance Team on matters relating to confidentiality and patient information.
- Deputise for the Chair of the Information Governance Group.
- Agree and review policies regarding the protection and use of personal information.
- Agree and review protocols governing the disclosure of personal information to partner organisations.
- Make the final decision on issues that arise regarding the protection and use of personal information.

5.4. Data Protection Officer

The Data Protection Officer will:

- Provide support, advice and assurance of data protection compliance across the Trust.
- Maintain expert knowledge of data protection law and practices and how they apply to the business of the Trust.
- Be involved properly and in a timely manner in all issues relating to data protection.
- Support programmes of work from the beginning to ensure that data protection is addressed by default and in the design of new systems and information processes, ensuring the completion of data protection impact assessments (DPIA) when necessary and consulting with the ICO where the proposed processing is high risk.
- Be available to be contacted directly by data subjects.
- Develop and advise senior management on the development and establishment of policies, procedures and other measures to ensure compliance with the data protection legislation.
- Monitor compliance with these measures and provide reports to the highest management level.
- Be the first Trust point of contact for the Information Commissioner's Office and co-operate with any matter relating to data protection compliance including breach management.

5.5. Information Governance Group

The Information Governance Group will:

- Ensure that the Trust has effective policies and management arrangements covering all aspects of Information Governance in line with national guidance and legislation.
- Perform 'horizon scanning' to look for new developments and changes across the information governance landscape.
- Discuss changes in information governance legislation, policy and guidance assessing the impact on the Trust, escalating these to the BeDigital Group as appropriate.
- Ensure that the Trust is meeting the UK General Data Protection Regulation/Data Protection Act 2018 and monitor performance to ensure compliance against the approved plan, taking action as required.
- Ensure that the Trust undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements; including the relevant Data Security and Protection (DSP) toolkit standards specifically Information Assets.
- Ensure the Trust continues to meet the compliance requirements of the Data Security and Protection (DSP) toolkit. To sign off an annual central return on the DSP toolkit that is

signed off by the Board.
- Establish an annual IG work and audit programme, secure the necessary implementation resources and monitor the implementation of that plan.
- Ensure that the Trust's approach to information handling is communicated to all staff and made available to the public.
- Co-ordinate the activities of staff with data protection, confidentiality, security, information quality, records management and freedom of information responsibilities.
- Monitor the Trust's information handling activities to ensure compliance with law and guidance taking action as required to ensure compliance.
- Ensure information governance training is provided to staff in line with national guidance.
- Receive reports and request action where necessary from the Clinical Systems Change Authority Group for major Trust systems.
- Receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action.
- Monitor compliance with action plans arising from incidents/audits.
- Report to the BeDigital Group for assurance purposes.
- Produce an annual report and annual objective to the BeDigital Group.
- Escalate significant concerns to the Executive Management Team.

The functions of the Group will be reviewed annually.

5.6. Information Governance Team

As directed by the Data Protection Officer, the Information Governance Team will:

- Support the Caldicott Guardian, Senior Information Risk Owner and Data Protection Officer in implementing the Trust Data Protection and Confidentiality Action Plan.
- Keep up to date on developments in relation to Confidentiality and Data Protection on a local, patch wide and national level and advise on the implications for the Trust.
- Develop, gain agreement and maintain Trust policies in respect of Confidentiality, Caldicott and Data Protection.
- Act as a focal point on detailed Data Protection, Caldicott and Confidentiality queries within the Trust.
- Maintain the Trust's entry on the Register of fee payers with the Information Commissioner; ensuring accuracy and updating were appropriate.
- Develop common actions and standards that can be applied across the local health community – in particular common information sharing agreements.
- Work with other agencies, for example Social Services and the Police to develop Information Sharing Agreements and ensure that the necessary policies and procedures are in place to underpin the agreements.
- Ensure a consistent approach is taken to implement data protection legislation.
- Develop, deliver and maintain an education, training and awareness strategy covering Data Protection, Caldicott, Confidentiality and Information Security.
- Liaise with local Data protection and Caldicott representatives concerning the development of patch wide action plans.
- Devise and produce quarterly performance reports in relation to the implementation and compliance with Data Protection, Confidentiality and Caldicott requirements.
- Produce progress reports against agreed scope of work to inform the Caldicott Guardian and Trust Information Governance Group.
- Complete annual external assessments for the Trust's performance against Confidentiality and Data Protection standards and produce organisation specific improvement plans.
- Work with each service area to help develop and improve their specific action plans.
- Develop local networks for sharing best practice and exploiting opportunities to work collaboratively.
- Manage the Information Asset Register
- Ensure that Information Asset Owners complete Information Asset Owner training.

- Identify and manage any risks in the Information Assets.

5.7. Information Asset Owners

Information Asset Owners will be responsible for key sets of information held manually and electronically. A register of Information Asset Owners is held centrally by Information Governance Team.

Information Asset Owners will:

- Act as nominated owner of one or more information assets of the Trust.
- Identify Information Asset Administrators to assist them with their duties, where this is appropriate and necessary.
- To complete a System Level Security Policy and Risk assessment to document, understand and monitor what information assets are held, for what purpose, how information is created, amended or added to, who has access to the information and why.
- To ensure that systems meets the Trusts information security standard.
- Identify information necessary in order to respond to incidents or recover from a disaster affecting the information asset.
- Take ownership via input to the Trusts Information Asset Register of their local asset control, risk assessment and management processes for the information assets they own, including the identification, review and prioritisation of perceived risk and oversight of actions agreed to mitigate those risks.
- Provide support to the Trust's Senior Information Risk Owner to maintain their awareness of the risks to all information assets that are owned by the Trust and for the Trust's overall risk reporting requirements and procedures.
- Ensure that relevant staff are aware of and comply with expected Information Governance working practices for the effective use of owned information assets.
- Provide a focal point for the resolution and/or discussion of risk issues affecting their information assets.
- Ensure that the Trust's requirements for the information incident identification, reporting, management and response apply to the information assets they own.
- Ensure new or proposed changes to Trust processes or information assets are identified and flagged with the Senior Information Risk Owner so that information security, confidentiality and data protection, and information quality requirements are defined at an early stage of the project.
- Undertake training in information risk management every two years.

5.8. Divisional General Managers

Divisional General Managers will be responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance.

5.9. General Management /Lead Clinicians

All managers will:

- Ensure that all current and future staff are instructed in their duty of confidentiality and security responsibilities.
- Disseminate to all staff the guidance, codes of conduct and information-sharing protocols referred to in Section 10 for obtaining, using and disclosing personal information. This is not an exhaustive list and managers will be advised when new guidance and protocols become available.
- Ensure that no unauthorised staff or other persons are allowed access to any of the Trust's computer systems or manually held information.
- Determine which individuals are to be given access to specific computer or manual systems. The level of access to specific systems should be on a job function need, independent of status.
- Ensure that staff changes affecting computer access (e.g. job function changes or leaving a

department) are notified via IT Service Desk in order that access may be updated.
- Complete the termination form for staff leaving the Trust so that access can be revoked.
- Monitor personal information to ensure that it is accurate and up to date.
- Ensure that any new process introduced ensure that confidentiality and data protection are considered by following the Data Protection Impact Assessment Standard Operating Procedure.

5.10. Employees, contract and agency staff and other people working on Trust premises

All employees, contract and agency staff and other people working on Trust premises have a duty to comply with the requirements of data protection legislation and the Caldicott Principles. Through appropriate training and responsible management, the above mentioned will:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal information. This includes guidance and code of conducts issued by professional bodies to which the employee is affiliated.
- Observe all information-sharing protocols in relation to the disclosure of information to provide care for individuals.
- Obtain and process personal information only for specified purposes.
- Only access personal information that is specifically required to carry out their work.
- Record information accurately in both manual and electronic records.
- Ensure that any personal information they hold is kept secure.
- Ensure that personal data is not disclosed in any form to any unauthorised third party.

6. Process

6.1. Collection and use of personal data (Lawful, fair and transparent)

The Trust's processes personal information in order to provide healthcare services for patients; to support and manage our employees, to maintain our accounts and records, to enable data matching under the national fraud initiative and for the use of CCTV systems for crime prevention.

The Trust will only collect the minimum information that is necessary to carry out operational needs or to comply with legal requirements.

The Trust will ensure a lawful basis for processing all personal data under Article 6 (UK GDPR) and will ensure a second legal basis special category data under Article 9 (UK GDPR).

When collecting patient data, service areas will ensure that individuals are adequately informed about the uses of their information by following Section 6 of the Confidentiality Code of Conduct.

All patients will be provided or directed to a copy of the currently approved patient privacy notice (short version) which can be found here. This is supported with a link to the full version privacy notice available on the internet and in Trust reception areas.

Under our Common law duty of confidentiality, there will be some cases when the Trust may only process personal information with the explicit consent of the individual. The Confidentiality Code of Conduct sets out circumstances when explicit consent is required.

When collecting other personal data (e.g. staff data) the Trust will provide the individual with a privacy notice that it is transparent about how their information is being processed. A staff privacy notice about the uses of staff information will be given at the start of employment with the Trust and is available on the Trust's intranet.

A Data Protection Impact Assessment (DPIA) will be completed on all projects, proposals or business changes that involve personal information. The Data Protection Impact Assessment Standard Operating Procedure will be followed.

6.2. Quality of personal information (Accuracy)

For personal information to be of use it is essential that it is accurate and up to date. The Trust will ensure the quality of information by:

- Validating and confirming information with data subjects.
- Informing data subjects about the importance of providing accurate information.
- Ensuring that all staff members who obtain and record patient information record it accurately, legibly and completely.
- Giving data subjects the opportunity to check information held about them.
- Encouraging data subjects to inform the Trust if any of their details have changed.
- Introducing monitoring procedures to check the accuracy of data.
- Incorporating validation processes into new systems.
- Maintain a high level of quality and timeliness in all data entered onto clinical records by following the Trust's Data Quality Policy.

6.3. Retention of personal information (Storage limitation)

The Trust will set retention periods for all personal information falling within the remit of data protection legislation.

Personal data will be retained and disposed of in accordance with NHS Records Management Code of Practice. Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)

6.4. Security of personal information (Integrity and confidentiality)

Personal information will be held and transferred in a secure manner in accordance with the Safe Haven Procedure and Information Security and Risk Policy.

Any breaches of confidentiality or security will be reported using Datix.

All incidents involving possible or actual breaches will be investigated. The Senior Information Risk Owner must be informed of all serious breaches.

Incidents will be reported to the Information Governance Group on a quarterly basis.

All breaches will be assessed and graded in accordance with the NHS Digital Guide to the Notification of Data Security and Protection Incidents.

Incidents reportable to the ICO will be recorded on the DSP Toolkit. Approval from the Senior Information Risk Owner, Caldicott Guardian and Data Protection Officer will be sought prior to reporting.

6.5. Individual rights

The Trust will uphold the rights of the data subject in respect of personal data processed by the Trust.

Be informed

The Trust will inform data subjects of their rights through privacy notices.

Right of access

Data subjects are entitled to copy of personal information held about them (subject access).

Subject access requests for patient records should be directed immediately to the Medical Records Administration Manager and will be dealt with in accordance with the Access to Health Records Policy.

Subject access requests for staff records should be directed to the Human Resources Department.

The Employee Information Access Guide will be followed.

Any request for other information should be directed to the Information Governance Team.

Compliance with the right of access for all data subjects will be monitored via the IG monitoring report.

Right to rectification
Requested for rectification will be dealt in line with the Access to Health Records Policy

Other rights include:

- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Further information regarding these rights can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Data Subjects wishing to exercise these rights should contact the IG Team in the first instance, however it should be noted that these rights do not apply to all personal data.

7. Consultation

Consultation has taken place with the Information Governance Group.

8. Implementation and monitoring

This policy will be disseminated by the method described in the Document Control Policy.

Information Governance training for staff will cover data protection legislation. The Information Governance Training Procedure will be followed.

This policy does not require additional financial resource.

Compliance with the data protection legislation will be monitored by the Information Governance Group via the annual completion of the DSP Toolkit.

Any breach will be managed via the Reporting Adverse Incident Reporting Policy and Procedure.

A quarterly report will be produced for the Information Governance Group detailing:

- Number and nature of Caldicott Function Log queries received.
- Details IG incidents reported including level and theme.
- Number and details of Freedom of Information requests and compliance with the legal timeframe.
- Compliance with IG training requirements.

- The number of Access to Records requests received and compliance with the legal timeframe.
- Storage for medical records.
- Lorenzo duplicate records.

- Confidentiality and information security complaints.
- Number of mail items returned via the Chief Information Officer.
- Details of IT security issues.
- Data quality compliance.
- IG communications to staff.
- SystmOne consent reports.
- Registration Authority activities.

9. Equality Impact Assessment

An Equality and Diversity Impact Assessment has been carried out on this document using the Trust-approved EIA.

10. Reference to supporting documentation

- UK General Data Protection Regulation (GDPR Keeling Schedule)
- Data Protection Act 2018 (Data Protection Act 2018 (legislation.gov.uk))
- National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs
- NHS Digital Guide to the Notification of Data Security and Protection Incidents
- Confidentiality: NHS Code of Practice 2003

11. Policies, procedures, protocols and guidelines

- Access to Health Records Policy
- Clinical Audit and Service Evaluation Policy and Procedure
- Community Adoption Record Keeping Procedure
- Confidentiality Code of Conduct
- Data Protection Procedure for Employment Records
- Data Quality Policy
- Electronic Communications and Internet Acceptable Use Procedure
- Enhanced Data Sharing Module (EDSM) SystmOne (SOP)
- Health and social care records policy
- Humber Information Sharing Charter
- Information Governance IT Forensic Investigation and Confidentiality Audit Procedures
- Information Governance Policy
- Information Governance Training Procedure
- Information Security and Risk Policy
- Information sharing with carers and significant others (SOP)
- Managing Health Records for Transgender Patients
- Photographing, Video and Audio Recording Procedure
- Patient objections to the creation or use of their health record Procedure
- Patient Online Access for GP Practices (SOP)
- Records management and information life cycle policy
- Data Protection Impact Assessment (SOP)
- Safe Haven Procedure
- Sharing information with the Police (SOP)

Appendix 1: Document Control Sheet

This document control sheet, when presented to an approving committee must be completed in full to provide assurance to the approving committee.

Document Type	Policy		
Document Purpose	This policy details how the Trust will comply with data protection legislation.		
Consultation/ Peer Review:	Date:	Group/Individual	
List in right hand columns consultation groups and dates			
Approving Committee:	IG Group	Date of Approval:	19 March 2024
Ratified at:	N/A (minor amendments)	Date of Ratification:	N/A (minor amendments)
Reviewed policy		Date of Approval	
Training Needs Analysis: (please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)	There are no training requirements for this document	Financial Resource Impact	There are no financial resource impacts
Equality Impact Assessment undertaken?	Yes [✓]	No [ ]	N/A [ ] Rationale:
Publication and Dissemination	Intranet [✓]	Internet [ ]	Staff Email [✓]
Master version held by:	Author [ ]	HealthAssure [✓]	
Implementation:	Describe implementation plans below – to be delivered by the Author:		
	Implementation will consist of: • Ratified policy to be shared with Executive Directors for sharing across directorates and with lead authors highlighting the new process • All staff email highlighting the key changes with a link to the full policy • Sub-committees to add approval of policies to their work-plan		
Monitoring and Compliance:	Monitoring and compliance of the policy will be evidenced through the process of consultation, approval and ratification of policies.		

Document Change History:			
Version Number/Name of procedural document this supersedes	Type of Change i.e. Review/Legislation	Date	Details of Change and approving group or Executive Lead (if done outside of the formal revision process)
		24/07/2002	*Original version ratified by Trust Management Team*
7.00	*Review*	*03/10/2011*	*Major changes, reviewed and re-written.*
7.01	*Review*	*03/09/2012*	*Updates approve by IG Committee 18/07/2012. Updated PIA form and addition of the Bribery Act.*
8.00	*Review*	*Sept 2015*	*Scope update to include all seconded staff, temporary staff and members of staff with an honorary contract or paid an honorarium. 7th Caldicott principles added. 4.3 removed the required for the Caldicott Guardian to specifically sign off the Confidentiality and Data Protection components of the IG Toolkit. 4.4 updated the role of the IG Committee in line with the current Terms of Reference and reduce to a summary of responsibilities. 4.5 combined the role of the Caldicott and Data Protection Officer and IG Lead. 5.1 updated in line with the current notification with*

			the Information Commissioner *5.5 updated in incorporate the HSCIC guidance for IG Serious Incident Requiring Investigation (SIRI).* *Appendix 3 – Procedure for the introduction of new processes, software or hardware removed to a standalone procedure.*
9.00	*Review*	*July 2018*	*Update to comply with General Data Protection Regulations (GDPR) and the Data Protection Act 2018. In particular detailing:* *1. the functions of the Data Protection Officer* *2. the functions of the IG Group* *3. processing, including lawfulness, fairness and transparency, accuracy, storage limitation, integrity and confidentiality and individual rights.*
9.01	*Review*	*May 2021*	*Updates include: information on how the Trust demonstrates compliance with the accountability principle. Addition of the eighth Caldicott principle. Updated all references to UK GDPR following our exit from the EU.* *Updated IG Group responsibility in line with the latest Terms of Reference. Removed reference to the Guidance for Informing Patients about the use of their information as this has been incorporated into Section 6 of Confidentiality Code of Conduct. Included the Caldicott Guardian and Data Protection Officer in the approval to report breaches to the ICO in line with current practice. Added that compliance with the "right of access" will be monitored by the IG monitoring report. Updated the details of the IG monitoring report in line with the current report.*
9.02	*Review –* *Minor amends*	*March 2024*	*Reporting Committee update to BeDigital Group. Role of the IG Group updated in line with the latest Terms of Reference. Role of the Information Asset Owner updated in line with the Information Security and Risk Policy. Details of the IG monitoring report updated in line with the current report. References and links updated. Approved at IG group by Director sign-off (Hilary Gledhill – 19 March 2024).*

Appendix 2: Equality Impact Assessment (EIA)

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: Caldicott and Data Protection Policy
2. EIA Reviewer (name, job title, base and contact details): Karen Robinson, Information Governance Officer, Mary Seacole Building, Willerby Hill. Tel. 01482 477856
3. Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other? Policy

Main Aims of the Document, Process or Service
To describe the roles, responsibilities and principles for ensuring that personal information is handled in a lawful and correct manner.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed?	How have you arrived at the equality impact score?
1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender re-assignment	Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory, Physical, Learning, Mental Health (and including cancer, HIV, multiple sclerosis)	Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.
Sex	Men/Male Women/Female	Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.
Marriage/Civil Partnership		Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Pregnancy / Maternity		Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.
Race	Colour Nationality Ethnic/national origins	Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.
Religion or Belief	All Religions Including lack of religion or belief and where belief includes any religious or philosophical belief	Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.
Sexual Orientation	Lesbian Gay Men Bisexual	Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.
Gender reassignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	Low	Any issues relating to this equality target group that have emerged from the Information Governance Issues Log. Any issues relating to this equality target group that have emerged from the PALS and Complaints reports supplied to the Information Governance Group. Any issues relating to the equality target group that have emerged from the IG Incident reports supplied to the Information Governance Group.

Summary

Please describe the main points/actions arising from your assessment that supports your decision. This is high level policy setting out how the Trust will comply with privacy legislation and would not have a negative effect on any of the above equality target groups.
EIA Reviewer: Karen Robinson, Information Governance Officer, Mary Seacole Building, Willerby Hill. 01482 477856
Date completed: 27/02/2024 | Signature: K Robinson