Tees, Esk and Wear Valleys
NHS Foundation Trust

Information Security and Risk Policy

IT-0010-v6

Status: Ratified
Document type: Policy

Contents

1 Why we need this policy

1.1 Purpose

This policy fits within the Trust's overall business risk framework and is needed to:

- Ensure the Trust complies with data protection and information governance law:
    - We have a duty of confidentiality to our patients and our colleagues;
    - We need to ensure that we have the correct and up to date information; it is available to those who have a genuine need to share it; and personal information is kept secure and confidential from those who do not have a genuine need to share it.
- Help staff keep information about individuals safe, secure, confidential and accurate:
    - This is a legal responsibility for the Trust and for all individuals who work within it;
    - We all, as individuals and as part of the Trust, have a duty of care in keeping person identifiable information (PII) safe, secure and accurate and available to only those who have a genuine need to share, access and use it.
- Give guidance to all Trust employees and agents on the process of identifying risks when dealing with confidential, restricted or sensitive information whether at rest, in use or in transit.

1.2 Objectives

This policy aims to support staff in identifying an acceptable level of risk when dealing with information. The policy also aims to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and risk management and explaining how they will be handled in the Trust.
- Introducing a consistent approach to information security and risk management, ensuring that all members of staff and, in particular, Information Asset Owners and Administrators, fully understand their own responsibilities.
- Creating and maintaining within the Trust a level of awareness of the need for information security and risk management as an integral part of the day to day business.
- Protecting information assets under the control of the Trust.
- Protecting the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant.
- Providing a consistent approach to risk management, where information risks are identified, analysed and dealt with in a timely and effective way.
- Identifying an acceptable level of information risk, beyond which escalation of risk management decisions is necessary.
- Safeguarding the Trust's information assets.
- Safeguarding the reputation of the Trust in the staff and service users mind through the safe and secure use of their information.

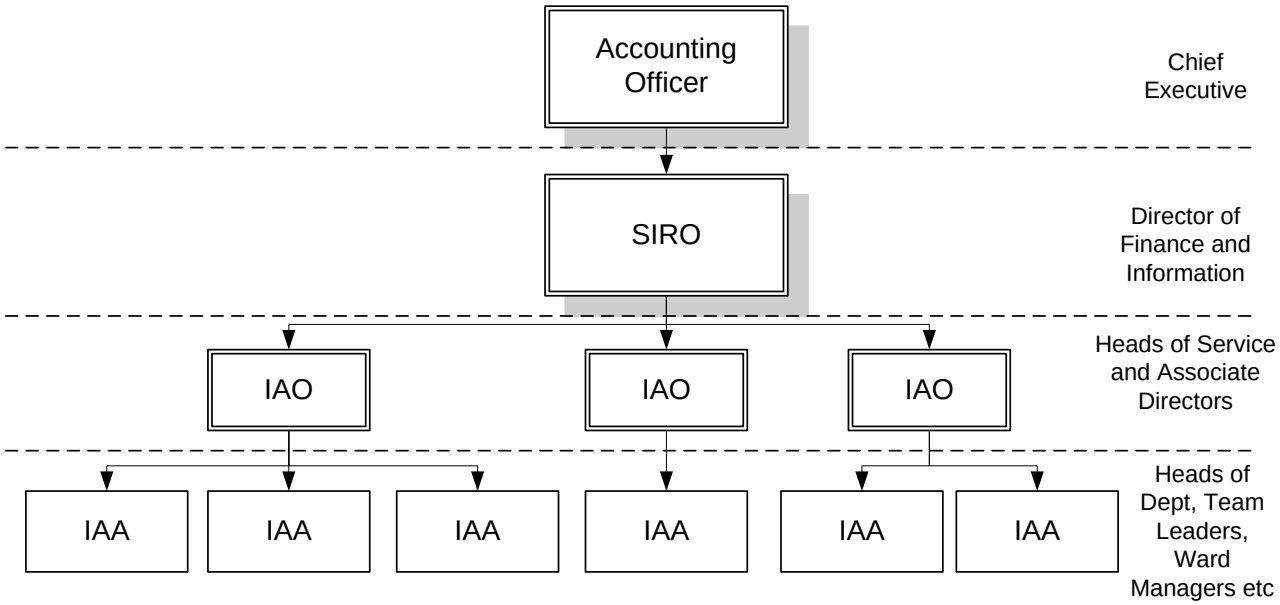
2 Scope

2.1 Who this policy applies to

This policy applies to:

- All information, information systems, networks, applications, locations and users of Tees, Esk and Wear Valleys NHS Foundation Trust. It also applies to any future information held by the Trust and any future equipment used to store or process the information.
- Every person working for the Trust, either as an employee, contractor, anyone on a work placement scheme or similar arrangement or working as an agent for the Trust, who handle business-sensitive and/or person-identifiable information on the Trust's behalf.

2.2 Information risk management structure



2.3 Roles and responsibilities

Role	Responsibility
Chief Executive	Ultimate responsibility for information security and risk management within the Trust.
Lead Information Security Officer	The day-to-day management and implementation of this policy and related procedures / associated policies.
Senior Information	• Coordinating the development and maintenance of information risk

Risk Owner (SIRO)	management policies, procedures and standards for the Trust. • The ongoing development and day-to-day management of the Trust's Risk Management Programme for information privacy and security. • The SIRO is supported by Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). • The SIRO advises the Chief Executive and the Trust Board on information risk management strategies and provide periodic reports and briefings on Program progress.
Information Asset Owner (IAO)	• To support the SIRO in ensuring that information risk assessments are performed on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency. • Submitting risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks.
Information Asset Administrator (IAA)	• To support the SIRO in ensuring that information risk assessments are performed on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency.
Line Managers	• Ensuring that their permanent and temporary staff and contractors are aware of:- o The information security policies applicable in their work areas; o Their personal responsibilities for information security; o How to access advice on information security matters. o How to identify risks to data confidentiality and how to reduce such risks. • Individually responsible for the security of their physical environments where information is processed or stored.
All staff	• Responsible for operational security of individual information systems and equipment they use, in line with this and other related Trust policies. • To be aware of risks in dealing with confidential or restricted information and to seek advice and guidance on how to deal with such risks, in line with Trust policies. • To be alert to any risk of accidentally revealing confidential or restricted information. Each user also needs to be on guard against unauthorized attempts to access information confidential or restricted information • Complying with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so will result in disciplinary action. • Complying with the security requirements identified within the relevant system specific policy (e.g. PARIS, ESR etc.)
External contractors	• External contractors needing access to the Trust information systems must have a current contract in place and will ensure that their staff comply with all trust security policies.

Incident Investigations Officer	• Investigate information incidents and report to the Information Security Officer.
System Administrators	• All administrators of systems that hold and/or process person identifiable information are required to sign an agreement which acknowledges their enhanced privileges and holds them accountable to the highest standards of use.

3 Policy

3.1 Security and risk

3.1.1 Management of security and risk

The Director of Finance, Information and Estates as the SIRO is responsible to the Board of the Trust. The Information Security officer has day to day responsibility for the Trust.

3.1.2 Information risk assessments

Information risk assessments will be done in line with the Organisational Risk Management Policy. Information security risks will be identified as incidents and managed by the Information Department with the aid of the Lead Information Security Officer.

Risk assessment will consider potential impacts on the confidentiality, integrity and availability of systems and data, and the likelihood of those impacts occurring.

In assessing the appropriate level of security, account is taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

As required by the Data Protection Act 2018 (GDPR), the Trust has embedded the process for undertaking a Data Protection Impact Assessment (DPIA) for all new systems and changes to existing systems. The DPIA process includes risk assessment and is documented in the DPIA Procedure.

All new Trust equipment that is used to store or transfer person-identifiable or business-sensitive data undergoes a standardised risk assessment.

3.1.3 Information security incidents and weaknesses

All information security events, near misses and suspected weaknesses are to be reported to the Information Security Officer. All information security events will be reported on Datix Web as soon as practicable to enable them to be investigated.

Decisions regarding the management of weaknesses and risks identified through the information risk assessment process are the responsibility of Digital Transformation and Safety Board. The implementation of technical and organisational measures to mitigate risk is monitored by the Cyber Security Group (see 3.2).

3.1.4 Business continuity and disaster recovery plans

Business continuity and disaster recovery plans will be maintained by the system owner. System specific policies must also include this requirement. Plans are developed with information security

standards included and are tested annually as a requirement of the Data Security and Protection Toolkit.

3.2 Cyber Security and technical measures

Cyber Security is increasing in importance, particularly because of new technology and ways of working. As a result of these advances, NHS Digital have produced the Digital Security and Protection Toolkit which focusses on Cyber Security and advances in technology.

The Trust has created a Cyber Security Group which meets on a monthly basis and assesses any issues and risks which have been noted, any updates or patches needed to Trust systems and any incidents which have occurred due to technical concerns.

Cyber Security Group monitors the implementation of CareCert (Care Computer Emergency Response) notifications which are received on a weekly basis. These are issued by NHS Digital to support health and social care organisations in responding effectively and safely to cyber security threats. The Cyber Security Group discusses these alerts and the ways in which to disseminate them throughout our network if they are applicable to any of the Trust systems. The group provides assurance of the governance of all of the technical measures taken by the Trust to adhere to the toolkit and maintain a high level of Cyber Security.

Digital Transformation and Safety Board will undertake a review of cyber security risk and include on the Board Assurance Framework the top 3 cyber risks.

3.3 Staff training and contracts

3.3.1 Information security and risk awareness training

All users **must** receive information governance training including information security and risk awareness as described in the Learning and Development Policy appendix 1**.**

Training is part of induction and is also refreshed annually or when there are changes to systems or legislation. The Trust has processes in place where individuals fail to apply the organisation's policies and practices.

3.3.2 Contracts of employments

All staff **must** remember that information security and management of risk is part of our terms and conditions of employment. This means we each have a responsibility to keep personal and restricted information confidential.

3.4 Security of assets

3.4.1 Control of assets

All information assets will be controlled by an Information Asset Administrator (see 2.2) who is responsible for maintaining a register of all IT equipment within their area.

The IAA must agree in advance the transfer of mobile devices such as smartphones to other staff and update the asset register accordingly. This is imperative so the mobile device can be remotely

wiped of information and/or barred from the Trust network. If the device is lost, the person named as owner on the asset register will be deemed liable.

3.4.2 Equipment security

All equipment will be physically protected from damage, loss or other hazards at all times including information transfer. Staff are responsible for protecting the assets under their control whilst the Trust retains responsibility for static assets.

3.4.3 Computer and network procedures

Information Department is responsible for maintaining IT systems and networks, adhering to authorised procedures and best practice. In the event that operation and maintenance of Trust systems and networks outside of authorised procedures is needed, e.g. in response to an incident, disaster recovery and business continuity processes will be followed. Any change to IT systems and networks that does not follow authorised procedures will be considered to be an information incident and managed as such.

3.4.4 Portable media

Any portable media must be Trust approved and virus checked. Staff must only use Trust purchased equipment and encrypted laptops, smart phones and data keys for business purposes.

You must not introduce any portable media - other than those provided and explicitly approved by the Trust – to the Trust's network. Trust approved equipment will always be security marked to show that it is owned by the Trust.

USB ports are locked down to only those portable media devices where a legitimate business need has been identified and agreed, and which are recorded on the Trust's central asset register.

3.4.5 Laptops

Trust issued laptops and tablets must be transported within the locked boot of the car. When travelling on public transport, extra care should be taken to ensure they are not left behind. Should it be necessary for them to be transported to the staff member's home overnight, laptops should be stored within the home out of plain sight, preferably within a cupboard or wardrobe.

3.5 Access controls

3.5.1 User access control

Only those with a justified and authorised need will be given access to restricted areas, e.g. server rooms. Access to restricted areas by non-authorised staff will be considered to be an information incident and managed as such.

3.5.2 Confidentiality

Access to confidential information or restricted information will be given on a need to know basis.

Storing Information on a Trust PC - no information should be stored on the hard drive (base unit or C drive) of a desk top computer. This is because the information on that hard drive is not encrypted, so can be viewed by anyone logged onto the computer who can access the C Drive, no matter who they are. This could cause a breach of information in two ways: firstly, the person who could then view the information may not have the legal requirement to be able to access the

information, therefore do not have a need to know. Secondly, should the computer be stolen, or accessed by a disgruntled member of staff, they would be able to get the information and use it in whatever ways they like. This would cause a breach which would at the very least, bring the Trust into disrepute and may, depending on the amount, type and number of pieces of information, be subject to scrutiny by the Information Commissioners Office.

Storing information on a laptop – All Trust laptops are encrypted to the NHS standard of AES 256. This means that even if the laptop is stolen, the thief could not get onto the hard drive (C drive) of the laptop as they would not have the credentials (i.e. log in and password) to pass through the encryption to the information behind. A stolen laptop must be reported on Datix and logged with the information service desk as soon as possible. It can then be banned from our network; should the laptop be found and recovered, it can then be added back into the network. Information is allowed to be stored on the hard drive/C drive of a Trust laptop as it is encrypted; however, information should only kept there for a short time as no one piece of equipment should be the sole source of information in case of corruption or loss. Once docked, or if wifi is available, the information should be transferred to the required network drive, either the home drive if in draft, or the shared drive should others need access.

Other IT equipment – this includes memory sticks, cameras, Dictaphones etc. All of these items must be encrypted where possible. Again, memory sticks and Dictaphones are encrypted to NHS standards but cameras can hold SD cards. The cameras themselves cannot be encrypted and only in some cases, will the SD card be encrypted. Local procedures in place where these cameras are used must state in the instructions for use that the SD card is removed from the camera, and the information stored on a nominated place on the network, immediately the camera has finished being used. Likewise, with all other portable information storage equipment, information should be stored on them for the least amount of time possible and should be transferred to the network at the soonest possible stage so that the information can be backed up by the Trust systems.

3.5.3 Computer access control

You **must** have a legitimate reason to use the Trust's computing facilities. This means you can only access confidential information if you have a genuine reason such as patient care or to progress the business of the Trust. If you do not have a genuine reason, you will be subject to the Trust disciplinary procedure.

3.5.4 Application access control

There must be a business need for access to business systems, and authorisation will depend on the availability of licenses for the software being used.

3.5.5 Monitoring system access and use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis. Any monitoring will be undertaken in accordance with the Regulations of Investigatory Powers Act, the Human Rights Act and the Data Protection Act 2018 (GDPR).

3.6 Moving sensitive information

Where service users' paper records need to be transported, please refer to the Trust's procedure for moving records and other sensitive information.

3.6.1 Classification of sensitive information

Information will be classified as follows:

- **NHS Confidential:** will be used for patients' clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies (paper/soft copy and electronic).
- **NHS Restricted:** will be used to mark all other sensitive information such as financial and contractual records. This includes information stored on computers, printed out or written, sent by fax or stored on disk etc.

NHS Restricted documents must be stored in lockable cabinets.

3.6.2 Encryption

It is a legal requirement that **PII** is **not sent** from the Trust to any external recipient **unless** the information is **encrypted to the NHS Standard of AES256**

A matrix of all approved encrypted email addresses is available in the NHSmail procedure. The procedure also describes how to send PII to a non-secure email address using the [secure] process (this is also described in the Communicating with Service Users Procedure). The Trust also allows the use of Egress for any large file transfers outside of NHSmail.

- In any other circumstance, you must seek advice before sending the confidential information:
  - From the Information Department's Compliance Team tewv.informationsecurity@tewv.nhs to identify a secure process;
  - From Information Governance if this is a new data flow and an information sharing agreement needs to be put in place.

3.6.3 Data transfer and sharing

Only authorised staff may be involved in the process of transferring batched or bulk person identifiable information (PII) by means of portable electronic media.

Contact the Information Department or Trust Information Security Officer for further guidance on permitted media.

Bulk PII is defined by the NHS Digital as either one piece of data that contains more than 50 pieces of PII or more than 50 separate pieces of data containing PII. If large quantities of paper or electronic data need to be transferred for any reason, you must contact your senior manager to gain permission.

3.6.4 Transfers of personal information outside of the UK

A transfer of personal data to another country or international organisation that is covered by the GDPR (i.e. within the EEA) does not require any specific authorisation providing that the transfer process follows Trust data security requirements.

A transfer of personal data to any other country must be discussed with the Trust's Data Protection Officer to agree how the data will be safeguarded.

3.6.5 NHSmail

Only a Trust-issued NHSmail account must be used. Web based emails (such as hotmail) must **never** be used for Trust business or sending emails which contain PII.

3.7 Software and systems

3.7.1 Protection from malicious software

Users are prevented from installing software on Trust equipment. All requests for software installation are managed via the procurement process.

3.7.2 Accreditation of information systems

All new information systems must be Trust approved. A system specific policy (SSP) must be produced referencing security management specific responsibilities and, in particular, supplier support arrangements and business continuity and disaster recovery processes. The SSP must be approved by Heads of Information prior to implementation of the system.

3.7.3 System change control

Changes to systems, policy or networks, including reviews and updates, must be reviewed with the involvement of the Information Department and approved by Technical Change Board. All new information systems, applications and networks must include a security plan approved by the information department before starting live operation. The Maintenance of IT Systems Policy and Introduction or upgrade of Information Systems Procedure cover in detail the process to be followed for introducing new information systems or amendments to existing systems.

3.7.4 Software copyright

All information products **must** be licensed and approved. Users **must not** install software on Trust equipment without permission from the Information Department. Users breaching this requirement will be subject to disciplinary action.

4 Reporting

The Information Department and the Information Security Officer will report to the Cyber Security Group and Digital Transformation and Safety Board on Information Security and any related incidents as and when required.

5 Further information

Further information and advice on this policy can be obtained from the Information Security Officer or Information Governance Manager.

6 Definitions

Term	Definition
AES 256 encryption algorithm	A process for encrypting information.

Availability	Information must be available and delivered to the right person at the time it is needed.
Confidentiality	Access to data will be confined to those with delegate authority
Consequence	The outcome of an event or situation, e.g. loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Datix Web	The Trust system for logging incidents, risks and issues
IAA	Information Asset Administrator
IAO	Information Asset Owner
Integrity	Information must be complete and accurate. All systems, assets and networks must operate correctly and to specification.
ISO 27001	The International Standards Organisation guidelines for ensuring personally identifiable information is stored, processed and disclosed lawfully and correctly.
Likelihood	The probability of the risk event happening.
Personally Identifiable Information (PII)	PII is information that could enable a person's identity to be established by one means or another. This might be fairly explicit, such as an unusual surname or isolated postcode, or bits of different information which if taken together, could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.
Restricted Information	Information about the Trust that is confidential. This includes financial information or sensitive information about business plans.
Risk	The chance that damage, loss or injury will occur, which will impact on objectives. It is measured in terms of *consequence* and *likelihood*.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk Management	The culture, processes and structures that enable the effective management of potential opportunities and adverse effects.
Risk Management Process	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Risk Treatment	Selecting and implementing options for dealing with risk. Treatment options will involve one or a combination of the following: • Avoid the risk • Reduce the likelihood of occurrence • Reduce the consequences of occurrence • Transfer the risk • Retain/accept the risk
SIRO	Senior Information Risk Owner

7 Related documents

- Integrated Governance Strategy
- Information Governance Policy
- Information Asset Register Procedure
- Introduction or Upgrade of Information Systems Policy
- Information or Upgrade of Information Systems Procedure

8 How this policy will be implemented

- This policy will be published on the Trust's intranet and external website.
- Line managers will disseminate this policy to all Trust employees through a line management briefing. The SIRO will ensure the policy is being followed within the Trust.

8.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	Information Governance	1.5 hours	Annually
IAAs/IAOs	Information asset management	2 hours	Annually

9 How the implementation of this procedure will be monitored

Auditable Standard/Key Performance Indicators		Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Risk reporting	Quarterly/Information Risk Policy and Records Standards Manager	Digital Transformation and Safety Board
2	SIRO report	Annually/Information Risk Policy and Records Standards Manager	Digital Transformation and Safety Board Executive Management Team

10 References

- Data Protection Act 2018 (GDPR)
- Computer Misuse Act 1990
- Sexual Offences Act 2003
- Privacy and Electronic Communications Regulations Act 2003
- Confidentiality: NHS code of Practice 2014
- Regulatory and Investigative Powers Act 2000
- NHS Digital

11 Document control

Date of approval:	10 August 2020	
Next review date:	31 January 2025	
This document replaces:	IT-0010-v5.1 Information Security and Risk Policy	
Lead:	Name	Title
	Lynn Holtam	Information Security Officer
Members of working party:	Name	Title
	Lynn Holtam Andrea Shotton	Information Security Officer Information Compliance Manager
This document has been agreed and accepted by: (Director)	Name	Title
	Drew Kendall	Director of Finance and Information (Acting)
This document was approved by:	Name of committee/group	Date
	Digital Transformation and Safety Board	11 March 2020
This document was ratified by:	Name of committee/group	Date
	Gold Command	10 August 2020
An equality analysis was completed on this document on:	24 February 2020	

Change record

Version	Date	Amendment details	Status
4	Jan 2015	Added detail around bulk data and portable media/encryption following disestablishment of Portable Media and Encryption Policy	Withdrawn
4	Jan 2017	Review date extended 12 months	
5	Dec 2017	Reviewed and amended in line with GDPR: 3.1.2 – two additional paragraphs added 3.1.3 – one additional paragraph added 3.2 – new section re cyber security and technical measures 3.6.3 – new section re transfers of data outside the EEA	Withdrawn
5.1	May 2018	New section 3.4.5 re security of laptops	Withdrawn
6	Aug 2020	Full revision with minor amendments throughout.	Published
6	May 2023	Review date extended to 31 December 2023	Published
6	June 2024	Review date extended to 31 August 2024 (agreed Mar 2024)	Published
6	Aug 2024	Review date extended from 31 Aug 2024 to 31 Jan 2025	Published

Appendix 1 - Equality Analysis Screening Form

Please note; The Equality Analysis Policy and Equality Analysis Guidance can be found on InTouch on the policies page

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc.	Information Department					
Name of responsible person and job title	Lynn Holtam – Information Security Officer					
Name of working party, to include any other individuals, agencies or groups involved in this analysis	Andrea Shotton – Information Risk, Policy and Records Standards Manager					
Policy (document/service) name	Information security and risk policy					
Is the area being assessed a…	Policy/Strategy	X	Service/Business plan		Project	
	Procedure/Guidance				Code of practice	
	Other – Please state					
Geographical area covered	Trust-wide					
Aims and objectives	This policy fits within the Trust's overall business risk framework and is needed to: • Ensure the Trust obeys data protection and information governance law: • Help staff keep information about individuals safe, secure, confidential and accurate: • Give guidance to all Trust employees and agents on the process of identifying risks when dealing with confidential, restricted or sensitive information. This policy aims to manage information risk so that staff can identify an acceptable level of risk when dealing with information. The policy also aims to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust.					

Start date of Equality Analysis Screening	24 February 2020
End date of Equality Analysis Screening	24 February 2020

You must contact the EDHR team if you identify a negative impact. Please ring Sarah Jay on 0191 3336267/3046

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?					
The policy benefits all individuals and organisations whose sensitive and personal information the Trust holds, transfers or processes					
2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?					
Race (including Gypsy and Traveller)	No	**Disability** (includes physical, learning, mental health, sensory and medical disabilities)	No	**Sex** (Men, women and gender neutral etc.)	No
Gender reassignment (Transgender and gender identity)	No	**Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.)	No	**Age** (includes, young people, older people – people of all ages)	No
Religion or Belief (includes faith groups, atheism and philosophical belief's)	No	**Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave)	No	**Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners)	No

Yes – Please describe anticipated negative impact/s

No – Please describe any positive impacts/s

Adhering to the policy will impact positively as this will ensure the security of information relating to individuals, including sensitive information the Trust may hold relating to a person's protected characteristic(s)

3. Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.? **If 'No', why not?**	**Yes**	**X**	**No**	

Sources of Information may include: • Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc. • Investigation findings • Trust Strategic Direction • Data collection/analysis • National Guidance/Reports		• Staff grievances • Media • Community Consultation/Consultation Groups • Internal Consultation • Research • Other (Please state below)

4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Gender, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership

Yes – Please describe the engagement and involvement that has taken place

Trust-wide consultation when developing the policy

No – Please describe future plans that you may have to engage and involve people from different groups

5. As part of this equality analysis have any training needs/service needs been identified?					
No	Please describe the identified training needs/service needs below				
A training need has been identified for;					
Trust staff	No	Service users	No	Contractors or other outside agencies	No
Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so					
The completed EA has been signed off by: You the Policy owner/manager: Type name: Lynn Holtam				Date: 24/02/2020	
Your reporting (line) manager: Type name: Andrea Shottom				Date: 24/02/2020	
If you need further advice or information on equality analysis, the EDHR team host surgeries to support you in this process, to book on and find out more please call: 0191 3336267/3046					

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
Signature:		Andrea Shotton	