Mersey Care NHS
NHS Foundation Trust

Policy Number	IT02
Policy Name	IM & T Security Policy
Policy Type	Trust-Wide Non –Clinical
Accountable Director	Director of Informatics and Performance Improvement
Author	IM&T Security Manager
Recommending Committee	Joint SIRO/Information Governance & Caldicott Committee
Approving Committee	Acquisition Steering Group
Date Originally Approved	December 2015 (Reviewed July 2016)
Next Review Date	December 2017

This document is a valid document, however due to organisation change some references to organisations, organisational structures and roles have now been superseded. The table below provides a list of the terminology used in this document and what it has been replaced with. When reading this document please take account of the terminology changes on this front cover

Terminology used in this Document	New terminology when reading this Document
Mersey Care NHS Trust	Mersey Care NHS Foundation Trust
Executive Director of Finance	Director of Informatics and Performance Improvement
Trust Board	Board of Directors

Mersey Care NHS
NHS Trust

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

IM&T Security Policy

Policy Number:	**IT02**
Scope of this Document:	**All Staff / Service Users / Carers / Volunteers**
Recommending Committee:	**Joint SIRO/Information Governance & Caldicott Committee**
Approving Committee:	**Executive Committee**
Date Ratified:	**December 2015**
Next Review Date (by):	**December 2017**
Version Number:	**2016 – Version 3**
Lead Executive Directors:	**Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO)**
Lead Author(s):	**IM&T Security Manager**

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

2016 – Version 3

Quality, recovery and wellbeing at the heart of everything we do

Mersey Care NHS Trust

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

IM&T SECURITY POLICY

Further information about this document:

Document name	**IM&T SECURITY POLICY (IT02)**
Document summary	**To identify and secure all Trust assets and ensure a secure and reliable system for the transference, manipulation and storage of Trust information. Identify and comply with national policies, laws and legislations**
Author(s) Contact(s) for further information about this document	**Mark Williams** **IM&T Security Manager** **Telephone: 0151 426 4031** **Email: mark.williams@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Trust** **Trust Headquarters** **V7 Building** **Kings Business Park** **Prescot** **L34 1PJ** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**SS01 – Social Netwroking Secruity Standard** **SS02 – Mobile working and Mobile Devices Security Standard** **SS03 – Internet and Email Security** **SS04 – User Account Investigation Secuiry Standard** **SS05 – Service User Internet Use Security Standard** **SS06 – Network Account Management Security Standard** **SS07 –Servuce User Access to the Internet (Specialist Learning Disabilities Division Only)** **SA03 – Policy & Procedure for the Reporting, management and Review of Adverse Incidents** **SA02 – Risk Management Policy & Strategy** **IT12 – Information Governance Policy**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
Consultation Draft	Circulated to Stakeholders for Comment	07 December 2015
Review of Policy	Circulated to Stakeholders for Comment	July 2016

SUPPORTING STATEMENTS – this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and vulnerable adults, including:

- being alert to the possibility of child/vulnerable adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable 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/vulnerable 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 vulnerable adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey 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

Mersey 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, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/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.

Mersey 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.

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

Contents

1 PURPOSE AND RATIONALE

1.1 **Purpose -** Mersey Care NHS Foundation Trust (from hereon know as "the Trust") recognizes the importance of its information and information systems for the transference, manipulation and storage of information to ensure business continuity. Through this policy, government laws and legislations (see section 5 Reference Documents) the Trust will identify and adopt structured security procedures for the Trust's information systems. The policy will ensure the Trust assets are available as and when required, adhering to the Trusts business objectives. The confidentiality to protect information from unauthorised access and disclosure. The integrity to protect its information from unauthorised or accidental modification ensuring accuracy and completeness of its information assets.

1.2 **Rationale** – Trust Staff are bound by the confidentiality and security policies set by the NHS, and by the common law duty to maintain confidentiality concerning the data and information they use as part of their everyday work within the NHS.

2 OUTCOME FOCUSED AIMS AND OBJECTIVES

2.1 For this IM&T Security Policy the aims and objectives are as follows:

(a) To protect all the information held by Mersey Care NHS Foundation Trust from all threats – internal and external, deliberate or accidental – to ensure business continuity including public access to information, guarantee the integrity and aithenticity of the records held. Information takes on many forms and includes data printed or written on paper, stored electronically or on tape, sent by post or electronic means, or spoken in conversation.

3 SCOPE

3.1 As a **Trust-wide non-clinical** document**,** this policy applies to all staff employed by Mersey Care (whether on a temporary or a permanent contract) Service Users, Carers and voluntary personnel.

3.2 All information that is created, processed, stored or transmitted or received during the course of the Trust's business activity is an asset of the organisation and as such is governed by this policy and the Confidentiality NHS Code of Practice (see section 5 Reference documents). This security policy covers all Trust owned I.T. systems and information communicated and managed by these IT systems. This policy applies to all Trust employees or other persons working for the Trust or whilst engaged on or involved in any Trust business and Service Users while using the Trust's computers. The policy applies to all Trust sites and places of work (including home) that are used to conduct the Trust business. This policy must be adhered to at all times. Failure to comply with this policy may lead to the Trust's disciplinary policy being invoked.

4 DEFINITIONS

4.1 The relevant terms and their definitions (within the context of this policy document) are outlined below:

Table 1: Definitions

Term	Definition
Confidentiality of Information	Person-identifiable, sensitive or otherwise valuable information will be protected against unauthorised access and disclosure.
Information Assets	Any information that is stored physically or electronically, transmitted across networks or telephone lines, sent by fax, spoken in conversations or printed.
Integrity of Information	Safeguards to protect against unauthorised modification and destruction of information.
Physical, Logical, environment and communications security	Controls to prevent unauthorised access, damage and interference to IM&T services and clinical records.
Infrastructure	Computers, systems, networks, cabling and other devices which make up the estate of information management in Mersey Care's estate.
Forensic Readiness	The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption or cost.
Cyber Security	Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies Cyber Security.
Security Standards	Security Standards are addendums to this policy and should be read/understood and fully adhered to as part of this policy. Security Standards are approved by the Joint Information Governance & Caldicot Committee, these standards allow for rapid changes to be implemented to account for quick changes in technology and legislation.

5 DUTIES

5.1 **Board of Directors –** The Trust will ensure that its information systems, applications and networks are available when needed; they can be accessed only by legitimate Users and should contain complete and accurate information. The information systems, applications and networks must also be able to withstand or recover from threats to their availability, integrity and confidentiality. To satisfy this, The Trust will undertake to the following:

5.2 Protect all hardware, software and information assets under its control. This will be achieved through compliance with Department of Health standards.

5.3 Provide both effective and cost-effective protection that is commensurate with the risks to its assets.

5.4 Implement the Information Security Policy in a consistent, timely and cost effective manner.

5.5 Where relevant, The Trust will comply with:

Access to Health Records Act 1990
Computer Misuse Act 1990
The Data Protection Act 1998
The Human Rights Act 1998
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Health & Social Care Act 2008
Equality Act 2010

5.6 **Caldicott Guardian** the Trust's Caldicott Guardian has a particular responsibility in ensuring that a robust framework to comply with all legislation is in place across the Trust. It is the responsibility of the Caldicott Guardian to ensure that ever member of staff within the Trust complies with all requirements of Information Governance, which is driven by various legislation and guidelines issued by the Department of Health and other sources.

5.7 **The Senior Information Risk Owner** is responsible for ensuring that the Trust manages its information assets securely and has taken appropriate action to mitigate against any data loss/data breach incidents and that all data loss/data breach incidents are monitored and reviewed.

5.8 **Director of Informatics & Performance Improvement** has designated responsibility for the SIRO as and when required.

5.9 **Information Governance Manager & Information Governance Committee**
The Information Governance Manager is responsible for ensuring that the Trust is working within the legal framework of the Data Protection Act, Freedom of Information Act, NHS Code of Practice for Records Management, NHS Code of Practice for Confidentiality, Information Governance Standards. The Information Governance Manager is the trust designated individual who liaises with the Information Commissioners Office. The Information Governance and Caldicott Committee ensure that the Trust operates within the Information Governance framework and is accountable to the Trust Executive Committee.

5.10 **IM&T Security Manager** – Will create and update the Trusts Cyber Security Awareness training for all staff.

5.11 The IM&T Security Manager will provide support to the Trusts Information Asset owners/administrators in providing security risks assessments for the assets and escalate these to the Joint SIRO & Caldicott Sub-Committee for consideration.

5.12 The IM&T Security Manger will provide regular reports on the Trusts IT Systems to demonstrate a significant level of assurance. All new Information Assets will be fully risk assessed and escalated to the Joint SIRO & Caldicott Sub-Committee prior to full implementation.

5.13 **Information Asset Owners** - The IAOs must be trained on appointment. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the SIRO annually on the security and use of their asset.

5.14 IAOs must formally review the risks to the confidentiality, integrity and availability of their information assets, including those in their delivery chain, at a minimum once a year and Implement proportionate responses.

5.15 **Information Asset Administrators** – Information Asset Administrators ensure that policies and procedures are followed locally. Recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date.

5.16 **Line Managers** – Are directly responsible for ensuring the security of the organisation's assets, (that is information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations.

5.17 Ensuring that their staff are aware of their security responsibilities and comply with all Trust policies and procedures. They must also ensure that their staff has completed the Cyber Security Awareness training annually.

5.18 **Project Managers** – Project Managers and others responsible for implementing systems are responsible for ensuring that effective security countermeasures are produced and implemented as part of any new systems project and ensuring that all releGvant system documentation relating to operating procedures and disaster recovery/business continuity plans are in place as part of the project.

5.19 Ensure that all information systems, applications and networks are approved by The Joint SIRO & Caldicott Sub-Committee and in conjunction with the Trust, before they commence operation, and that approval is appropriately documented.

5.20 Ensure that the relevant Project or System Manager reviews changes to the security of any information system, application or network. In addition, all such changes must be reviewed and approved by The Joint SIRO & Caldicott Sub-Committee, and in conjunction with the Trust.

6 STAFF TRAINING

6.1 A sound working knowledge of information security purposes and practice is required by all staff that works for the Trust. This is in order to ensure business continuity, legal compliance and that patient, Service Users and staff's rights under the law are facilitated and upheld. To achieve this the Trust provides a mandatory (compulsory) training programme for all staff that process or handle confidential or business critical information or service or maintain information systems.

7 CONFIDENTIALITY

7.1 If a document is highly confidential or sensitive in nature, it must stored in a private directory or an equivalent password protected directory. It should be noted that documents in common directories can be accessed by other employees.

7.2 All data stored within the Trust is subject to the Data Protection Act 1998. Any person copying data from a source and storing it on a 'Home' network drive will need to adhere to the Act's stated principles with that data, in particular:

7.3 Principle 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

7.4 Principle 4. Personal data shall be accurate and, where necessary, kept up to date.

7.5 Principle 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7.6 Principle 7 requires security for all personal data whether held on computer or in manual files. This includes physical security from unauthorised access as well as protection against accidental loss, destruction or damage.

7.7 Copies of confidential information should only be printed out as necessary, retrieved from the printer immediately and stored or destroyed in an appropriate manner (see section 2.10.1 of the Health Records Policy).

7.8 Staff that work between the standard environment and High Secure need to be aware at all times of what printers they have set. It is unacceptable to print High Secure documentation to a standard environment printer and vice versa.

7.9 Clinically confidential information is part of the Health Record and should be transferred to the appropriate electronic or paper based system (Please refer to the Trust policy and procedure for Health Records) http://www.merseycare.nhs.uk/about-us/policies-and-procedures

7.10 Staff must not leave documents containing Trust patient/staff information open on their monitor. They must always logout or lock any computer when leaving their desk. When possible position their monitor as to not let other members of staff over see what is on their screen.

8 EMAIL

8.1 All information relating to Email is contained within SS03 Internet and Email Security Standard. This Standard must be read, understood and adhered to as part of this Policy.

SS03 Internet and Email Security Standard

9 INTERNET

9.1 All information relating to the Internet is contained within SS03 Internet and Email Security Standard. This Standard must be read, understood and adhered to as part of this Policy.

SS03 Internet and Email Security Standard

10 SOCIAL MEDIA

10.1 All information relating to Social Media is contained within SS01 Internet and Email Security Standard. This Standard must be read, understood and adhered to as part of this Policy.

SS01 Social Networking Security Standard

11 USER ACCOUNT INVESTIGATIONS

11.1 All information relating to User Account Investigations is contained within SS01 Internet and Email Security Standard. This Standard must be read, understood and adhered to as part of this Policy.

SS04 User Account Investigations Security Standard

12 REMOTE WORKING & MOBILE DEVICES

12.1 All information relating to Remote Working & Mobile Devices is contained within SS02 Remote Working & Mobile Devices Security Standard. This Standard must be read, understood and adhered to as part of this Policy.

SS02 Remote Working & Mobile Devices Security Standard

13 NETWORK ACCOUNT MANAGEMENT SECURITY STANDARD

13.1 All information relating to Network Account Management is contained within SS06 Network Account Management Security Standard. This Standard must be read, understood and adhered to as part of this Policy.

SS06 Network Account Management Security Standard

14 SERVICE USER INTERNET USE SECURITY STANDARD

14.1 All information relating to Service User Internet Use is contained within SS05 Service User Internet Use Security Standard. Specialist Learning Disabilities Division Service User Internet Use is contained within Service User Internet Access to the Internet document SS07. These Standards must be read, understood and adhered to as part of this Policy.

15 PASSWORD MANAGEMENT

15.1 Passwords are confidential information and must be treated as such. A password is only as secure as the person who knows it and as such the standards that must be adhered to are documented in SS06 Network Account Management Security standard. This Standard must be read, understood and adhered to as part of this Policy.

SS06 Network Account Management Security Standard

16 SECURITY INCIDENT HANDLING

16.1 The Trust recognises the risk of an incident occurring involving Trust I.T. systems and as such has put in place the following IT Security incident handling procedures.

16.2 An I.T. Security Incident can be described as any situation involving Information Technology systems or information that is stored, manipulated or communicated by or through these systems being affected in an adverse way either through controlled or uncontrolled circumstances which could result in:

a) Loss, damage or theft of information.

b) Disclosure of confidential information to unauthorised persons.

c) The integrity of I.T. systems or information being put at risk.

d) Availability of I.T. systems or information being put at risk.

16.3 The Trust recognises the importance of all I.T. related security incidents being handled using a structured, coherent and proven method, ensuring all incidents are handled in a consistent manner.

16.4 All IT related incidents will be processed through the Trust's Adverse Incidents Department to keep continuity on the handling of all incidents within the Trust.

16.5 **Incident Classification -** The Trust's Adverse Incident Department are responsible for classifying incidents. There are four levels of seriousness from "D" being least serious to "A" being most serious (see section 7.2 Reference documents "*Policy & Procedure for the Reporting, Management and Review of Adverse Incidents"*). These classes are measured using the *Adverse Incident Classification Matrix.*

Class D incidents can include but are not limited to:

a) Inappropriate use of e-mail.
b) Inappropriate use of internet access not causing the Trust any financial or adverse publicity.
c) Equipment failure with no loss of information or impact on Trust business functions.

Class C incidents can include but are not limited to:

a) Equipment failure which leads to service disruption

Class B incidents can include but are not limited to:

a) Loss of data, Illegal attempts to access trust networked services or breaches of information policies.

Class A incidents can include but are not limited to:

a) Permanent loss of data with failed backup or restore function.

16.6 **Reporting Incidents** - It is important to remember that although an incident class is initially decided

by the Adverse Incidents Department the incident class can be changed after an investigation into an incident.

16.7 Depending on the different types of incidents and their severity the following is a guideline on the actions that should be taken following an I.T. security related incident.

16.8 All I.T. security related incidents must be reported to the Adverse Incidents Department using the Adverse Incidents form. The form must be completed by the person who discovered the incident or who is affected by the incident. The form must be completed and sent within 24 hours of the incident occurring and sent directly to the Adverse Incidents Department.

16.9 The Adverse Incidents Department will progress the incident inline with the "*Policy & Procedure for the Reporting, Management and Review of Adverse Incidents".* The incident must be recorded on the Trust Incident Management System (DATIX).

16.10 The Adverse Incidents Department will then report all I.T. security related incidents to the I.T. Security Manager via email or phone who will log the incident on the Service Desk call logging system (Sostenuto).

16.11 If the incident was caused through a malicious act, the Adverse Incidents Department will contact the line manager of the member of staff who was responsible for the incident and will request that they contact the member of staff's HR manager who will progress the incident further and in line with HR procedures. Any further action will be taken up by the HR department under HR policies and procedures.

16.12 **Responding To An Incident** - The IM&T Security Manager will contact the Service Delivery Manager and the member of staff's manager to discuss the incident.

16.13 The IM&T Security Manager will contact the line manager to discuss the incident in relation to:

a) How the incident occurred

b) How the incident will be resolved

c) Actions needed to stop any future reoccurrence of the incident.

16.14 The I.T. Service Desk will issue a communication to all staff affected by an incident causing a service interruption.

16.15 If there has been loss, damage or theft to patient information the I.T. Security Manager will contact the Service Governance Department and the Caldicott Guardian.

16.16 If it is decided that access to I.T. systems needs to be removed, a request must come from the member of staff's manager or Head of Directorate unless there is a direct threat to the Trust systems, in which case the I.T. Security Manager or Operations Manager will authorise the removal of I.T. resources from the member of staff with immediate affect.

16.17 When an incident involving computer misuse occurs the IM&T Security Manager must investigate the member of staff's computer and/or computer accessories to collect any evidence needed for legal proceedings.

16.18 The I.T. department reserves the right to disconnect and disable a user's account if it is suspected that they are in breach of the IM&T Security policy pending an investigation.

17 CORPORATE PROCEDURE

17.1 This policy will be implemented through compliance with statuary requirements and legal obligations as per HSCIC guidelines and Caldicott guidelines. Through annual policy reviews, training in IT security awareness and IT security reviews.

18 BUSINESS CONTINUITY

18.1 The Trust is aware that some form of disaster may occur, and as such, all directorates/Information Asset Owners will implement and regularly update a business continuity management process. This will ensure that the Trust can counteract interruptions to normal activity and to protect critical processes from the effects of failures or damage, to vital services or facilities.

19 MONITORING AND COMPLIANCE

19.1 The policy will be monitored for effectiveness by measurement of the number of reported IT Security Incidents and also the IT Security linked IG Toolkit compliance scoring. Bi monthly reports are produced to the Joint SIRO/Information Governance & Caldicott Committee review and these are then escalated to the Executive Committee

20 DEVELOPMENT & CONSULTATION PROCESS

20.1 The Policy has been developed by the IM&T Security Manager. The Policy has been reviewed by the Director of Informatics and the Joint Information Governance and Caldicott Committee.

20.2 This policy and related Security Standards will be under continual development and consultation due to the nature of Information Technology and its constant evolvement with the introduction of new technologies.

20.3 The policy will also be reviewed on a 2 yearly basis.

21 SUPPORTING DOCUMENTS

List of Supporting Documents

Ref No	Name	Purpose
SS01	Social Networking Security Standard	
SS02	Mobile Working and Mobile Devices Security Standard	

Ref No	Name	Purpose
SS03	Internet and Email Security Standard	
SS04	User Account Investigations Security Standard	
SS05	Service User Internet Use Security Standard	
SS06	Network Account Management Security Standard	
SA03	Policy & Procedure for the Reporting, Management and Review of Adverse Incidents	
SA02	Risk management policy & strategy	
IT12	Information Governance Policy	

22 GLOSSARY OF TERMS

Glossary of Terms

Term	Description	Reference
BES	Blackberry Enterprise Server	
BMP	Bitmap / Picture files	
CDA	Compact Disk Audio / Music file	
CfH	Connecting for Health	
FTP	File Transport Protocol	
GIF	Graphics Interchange Format / Picture file	
Informatics Merseyside.	Health Informatics Service	
JPEG	Joint Photographic Experts Group / Picture file	
LAN	Local Area Network	
MP3	Moving Picture Experts Group Layer-3 Audio / Video / Audio file	
N3	New NHS National network	
NHS Net	NHS Network	
PDA	Personal Digital Assistant	
PII	Patient Identifiable Information	
Secure Token	Device that creates a secure password.	
TELNET	Telecommunications Network	
VPN	Virtual Private Network	
WAN	Wide Area Network	
WMA	Windows Media Audio/ Video Audio file	

Equality and Human Rights Analysis

Title: I M and T Security Policy
Area covered: Trust-wide Non Clinical

What are the intended outcomes of this work? To identify and secure all Trust assets and ensure a secure and reliable system for the transference, manipulation and storage of Trust information. Identify and comply with national policies, laws and legislations
Who will be affected? The policy directs staff. Service user's personal information protection.

Evidence

What evidence have you considered? Policy itself.
Disability Need to ensure that IM are aware of confidentiality /information security is maintained if specific disability reasonable adjustment is made re computer/data access systems are put in place for staff.
Sex Nothing found
Race Nothing found
Age Nothing found
Gender reassignment (including transgender) The Trust is assuring the protection of personal data
Sexual orientation Nothing found
Religion or belief Nothing found
Pregnancy and maternity . Nothing found

Carers Nothing found
Other identified groups Nothing found

Cross Cutting Inclusion of Equality Act within 5.5 page 7

Human Rights	Is there an impact? How this right could be protected?
Right to life (Article 2)	*Not engaged*
Right of freedom from inhuman and degrading treatment (Article 3)	*Not engaged*
Right to liberty (Article 5)	Not engaged
Right to a fair trial (Article 6)	Not engaged
Right to private and family life (Article 8)	This is supportive of this article
Right of freedom of religion or belief (Article 9)	Not engaged
Right to freedom of expression **Note: this does not include insulting language such as racism (Article 10)**	Not engaged
Right freedom from discrimination (Article 14)	Not engaged

Engagement and Involvement *detail any engagement and involvement that was completed inputting this together.*
There was no external engagement

Summary of Analysis

Eliminate discrimination, harassment and victimization

This policy is supportive of data protection and the prevention of data loss which may be of significant importance to people with protected characteristics.

Advance equality of opportunity

This policy recognises the specific issues for staff with disabilities.

Promote good relations between groups

The equality analysis process is supportive of relationships between groups and the prevention of breeches that may cause issues.

What is the overall impact?

This policy is supportive of Equality and Human Rights for staff and the people who use services.

Addressing the impact on equalities

The policy has specific guidance for staff and managers re Disability and specific systems to ensure access to systems the Trust has in place.

Action planning for improvement

Action in place within action plan

For the record

Name of persons who carried out this assessment:

Date assessment completed:

Name of responsible Director:

Date assessment was signed:

Action plan template

Category	Actions	Target date	Person responsible and their area of responsibility
Increasing accessibility	To include specific guidance re security assurances and guidance for systems provided to staff with disabilities.		Mark Williams
Legal requirements	To include Equality Act 5.5 page 7	March 1st	Mark Williams