NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON-CLINICAL DOCUMENT

Service User Internet Security Standard

Standard Number:	SS05
Scope of this Document:	All Staff/ Services Users
Recommending Committee:	Joint Information Governance & Caldicott Committee
Approving Committee:	Joint Information Governance & Caldicott Committee
Date Ratified:	February 2020
Next Review Date (by):	December 2021
Version Number:	Version 2
Lead Executive Director:	Executive Director of Finance
Lead Author(s):	IM&T Security Manager

TRUST-WIDE NON-CLINICAL DOCUMENT

2018 – Version 2

Striving for perfect care and a just culture

TRUST-WIDE NON-CLINICAL DOCUMENT

SERVICE USER INTERNET SECURITY STANDARD

Further information about this document:

Document name	**Service User Internet Use Security Standard SS05**
Document summary	**Trust Standard On the use of Internet and email**
Author(s) Contact(s) for further information about this document	**Mark Williams** **IM&T Security Manager** **Telephone: 0151 472 4031** **mark.williams@imerseyside.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Foundation Trust** **Trust Headquarters** **V7 Building** **Kings Business Park** **Prescot** **L34 1PJ** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IM&T Security Standard IT02**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

Version History:		
Draft	Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Cadicott Guardian	December 2015
Review	Informatics Merseyside ITSecurity	December 2017
Version 2		February 2020

SUPPORTING STATEMENTS –

Failure to adhere to the acceptable usage outlined in this Policy will be deemed as misconduct, any required deviation from these guidelines must be reviewed on an individual basis at the trusts discretion.

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 adults, including:

- being alert to the possibility of child/ adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/ adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/ adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust Standard 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** –At Mersey Care NHS Foundation Trust, communication plays an essential role in the conduct of our business. We value staff's ability to communicate with colleagues in the Trust, the wider NHS and associated agencies. Mersey Care NHS Foundation Trust invests substantially in information technology and communications systems which enable staff to work more efficiently and effectively and Trust's staff to use them responsibly. This standard has been established to ensure that where service users are enabled by staff to access and use the Internet on Trust premises this is done in a supervised and managed way. It is the responsibility of the individual directorates and line managers to ensure this procedure is adhered to by staff and service users.

1.2 **Rationale** – It is expected that all staff use the information technology Internet and communications facilities sensibly, professionally, lawfully, consistently with your duties, with respect for your colleagues and in accordance with Trust policy, the Email and Internet Use Policy and Mersey Care NHS Foundation Trust*'s* rules and procedures. The same general principles will apply to the access and use of the internet by service users on Trust premises.

This standard does not permit access to the internet for service users in High Secure and Medium Secure Services. Separate arrangements have been made for service users within medium and high secure environments.

2 OUTCOME FOCUSED AIMS AND OBJECTIVES

2.1 *For this Security Standard the aims and objectives are as follows:*

(a) To ensure the use of Internet and Email is carried out safely and securely, representing the Trust in a professional manner

(b) To ensure that service users understand the Trust's expectations for the use of the Internet.

(c) To ensure that service users use professional conduct on the Internet and do not misuse Trust resources.

(d) *To highlight that failure to comply with the requirements of this Standard, including non-compliance with the Computer Misuse Act 1990 and General Data Protection Regulations, or infringement of copyright, will be regarded as a serious offence, and access will be immediately revoked. Misuse will be reported to the senior executives of the Trust.*

3 SCOPE

This standard applies to:

3.1 All service users who are granted access to the Trust's Internet connection.

3.2 Trust staff that are responsible for monitoring the service user's access, account creation and deletion.

4 RESPONSIBILITIES

4.1 All service users are responsible for their own internet usage and must sign the declaration below to acknowledge they have read and understood this standard.

4.2 Service users are asked to be vigilant and report any suspected breaches of this standard immediately to a member of staff. Although the Trust believes that its approach to implementing the standard is flexible, firm measures are in place to guard against computer misuse or gross misconduct. Should a serious breach of this standard be made by a service user, it will be reported the Trust's executives

4.3 Examples of Gross misconduct and misuse include: (this list is not exhaustive)

a) Accessing, downloading and/or distributing pornographic or other offensive material. This may include racial, sexual material or derogatory information about others.

b) Accessing, downloading and/or distributing information of a discriminatory nature including sexual or racist material or information which is discriminatory towards other groups such as the disabled.

c) Deliberately or negligently downloading malware (such as viruses, spyware) which expose the Trust's IT security measures and expose Trust computer systems to risk of damage.

d) Deliberately breaching the Computer Misuse Act 1990 or the General Data Protection Regulations, for example, passing patient related data to inappropriate parties.

e) Downloading, storing and or using copyrighted materials or software such as music and video files, images or computer software.

f) Administering, supporting or moderating a 3rd party internet site such as discussion groups, fan sites or websites for a business.

5 STANDARDS PROCEDURES

5.1 Internet access for Domain service users will be controlled and monitored via the same processes and management systems as per Internet access for Mersey Care employees.

5.2 Service Users will be provided with the same levels of access to websites as per Mersey Care employee. The same restrictions to Adult, Offensive and inappropriate websites will apply However all other websites are accessible to both employees and Service Users and, like staff, service users must use the Internet in a responsible way.

5.3 Service Users will logon to the PC/Network to gain internet access via their own unique username and password so that the same monitoring and control of the internet can be maintained by Informatics Merseyside and reports on internet activity can be provided on a per username/service user basis.

5.4 The account used by Service Users to logon to the PC will only provide access to the Internet, MS Office applications such as Word and Power Point and not any other applications of systems on the computer or the ability to store or view data on the PC or Trust data storage areas.

5.5 Email accounts will not be provided to Service Users unless approved by the Chief Executive.

5.6 The ability to print from the Internet will be provided.

5.7 Service Users will be provided with their username and password to logon to the PC to gain Internet access.

5.8 Service Users must only logon to PCs and use the internet via their own personal accounts. Under no circumstances must Service Users use a Staff members account to connect to the PC and the Internet or use another service user's account.

5.9 It is the responsibility of the employee requesting the service account to ensure the service user is aware of the Internet use policy and has it explained to them. The service user must fully understand the policy and that it is their responsibility to comply with this policy, which is available from the Mersey Care website.

5.10 Before a new service user account is created, the requesting party will be sent a copy of this document alongside the Internet and Email security standard.

5.11 When a service user leaves the care of Mersey Care or no longer wishes to have a Mersey Care account, they should notify informatics Merseyside so that the service user account can be disabled. A Service User account that has not been used for a period of 6 months will be disabled.

5.12 If in the event of inappropriate activity on the PC or internet by the service user being discovered and/or the requirements of this procedures and policies not being applied by the Service User then at such point the Service User account may be disabled whilst further investigations take place. Depending on the scenario and severity of the breach of procedure then all Service User internet access may be Withheld whilst further investigations take place.

6 DECLARATION

By signing this declaration
You agree that you **have read and understood** the IM&T security policy and you agreed to be bound by its terms.

Print Name _____

Signature_____

Date___/___/___ (DD/MM/YY)