NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON-CLINICAL DOCUMENT

Internet and Email Security Standard

Standard Number:	**SS03**
Scope of this Document:	**All Staff**
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

INTERNET AND EMAIL SECURITY STANDARD

Further information about this document:

Document name	**Social Networking Security Standard SS03**
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 2967643** **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 IT Security	April 2018
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** – Internet and Email is an important part of the Trust's and the wider NHS communications system. Use of the installed systems/connections is for legitimate work related purposes only and is encouraged to improve the quality of work and productivity in patient care, research, operational matters, education and development.

1.2 **Rationale** – We must ensure that the increasing use of information technology maintains patient confidentiality, is not misused, and at the same time is secure and accurate. This Standard provides guidance on the Trust's expectations for the use of the internet and email.

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 the Trust's staff understand the Trust's expectations for the use of the Internet and/or email

(c) To ensure that Trust staff use professional conduct on the Internet and whilst using the email system, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of Trust resources, harassment, information and data security, and confidentiality.

(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 breach of discipline which will result in disciplinary action being taken. Although each case will be judged on its own merits, misuse of the Internet and email (or any misuse of computer systems) may be considered Gross Misconduct and lead to dismissal.*

(e) To ensure the Trust communicates using Internet and Email appropriately.

3 SCOPE

This standard applies to:

3.1 All full-time and part-time employees of the Trust, and non-executive directors, contracted third parties (including agency staff), Service users, locums, students and trainees, secondees and other staff on temporary placements with the Trust, and staff of partner organisations with approved access;

3.2 Other individuals and agencies who may gain access to data, such as volunteers, visiting professionals or researchers, and companies providing IT services to the Trust.

3.3 The use of the Trust's Internet or Email on any Trust owned device including Laptops, iPads, Tablets, Mobile Phones, Smart phones, Blackberries.

Please note the procedures and policies outlined in this Standard and any related Standard may be changed at any time. You will be alerted to this via established Trust communication routes such as team brief, weekly and monthly round up, intranet and internet.

4 RESPONSIBILITIES

4.1 All employees are responsible for their own internet usage and also have responsibility for the emails they send.

4.2 Employees are asked to be vigilant and report any suspected breaches of this standard immediately to their line manager or to HR as appropriate. 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 user, then disciplinary action may be taken.

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 Trusts 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.

g) Using the Trust's email system to conduct business not related to the Trust or as a private organisation.

h) Sending Personal Identifiable information without using the Trust's email encryption solution.

5 INTERNET USE

5.1 The Internet is a powerful information acquisition and dissemination tool that provides access to unique resources. The Trust reserves the right to restrict access to materials on the Internet where deemed appropriate. This will include access to pornographic and other sites considered offensive. Any restrictions to material by the Trust shall not be deemed to impose any duty on the Trust to regulate the content of material on the Internet. Furthermore, any lack of restriction does not mean that access to that material is authorised.

5.2 Use of the Internet is made available to employees for work duties, work-related educational purposes and work-related research purposes. Personal use of the internet is limited to lunch breaks and work breaks only – employees may not use the internet for personal use during otherwise working hours. While personal use is permitted during lunch and work breaks, this is only providing that the material

accessed is appropriate and not potentially offensive to others. Employees should regard this facility for personal use as a privilege that is only exercised in their own time, without detriment to their job, or the work of others, and not abused. Excessive or inappropriate use of the Internet, including violation of this Standard, may result in disciplinary action being taken and/or removal of facilities.

5.3 Accessing of pornographic and abusive or offensive material, including sites that may constitute unlawful discrimination on the grounds of race, disability or gender, is not permitted. Such actions will be regarded as gross misconduct and will result in summary dismissal.

5.4 The Trust reserves the right to block access to any sites it feels are contrary to Trust Policy/Security Standard or where the amount of data traffic generated adversely affects the Trust's business use of links to the Internet. This may include restricted access to social networking sites and heavy bandwidth sites such as streaming hosting sites.

5.5 Access to streaming media may be permitted if it is necessary for the role of the employee. Access to streaming requires approval form your line director only and can be requested via the Service Desk.

5.6 Employees within the Trust are permitted view only access to social networking sites however it is not permitted to post using Trust equipment. The only exception to this is where access to such sites is required for business purposes and this must be approved by your line director. For further information please see Social Networking Security Standard SS01.

5.7 Information obtained through the Internet may not be accurate, and the user must check the accuracy, adequacy or completeness of any such information. Furthermore, it is the responsibility of the user when using information obtained from the Internet to be aware of copyrighted material in accordance with the permission granted by the publisher.

5.8 The threat from viruses and security breaches from the use of the Internet are very real. Users must be aware that information and programs downloaded from the Internet may contain hidden code capable of destroying data or interfering with the network. Therefore, users must take great care and be vigilant if they are required, as part of their employment, to download or install any executable or program files from the Internet. Any executable program files not connected with an employee's duties must not be downloaded. All PC's accessing the Internet must have virus-checking software, which is installed by Informatics Merseyside. The use of a 'firewall' will protect the Trust from 'attacks' from outside the organisation.

5.9 All users of the Trust's Internet connection who supply their personal details, including credit card details, etc. whilst accessing web sites do so at their own risk. The Trust employs security measures to counteract some types of .malware or attempts to extract personal information but cannot guarantee protection against all threats and therefore the onus is on user vigilance.

5.10 All users of the Trust Internet connection are forbidden from downloading copyrighted material such as music or software as this is against the law.

6 EMAIL USE

6.1 Email is the electronic transfer of messages from one computer to another, whether this is within the Trust, NHS or with anyone throughout the world. The Trust Email system should be utilised as a formal communication system.

6.2 The NHS has created a secure infrastructure for the provision of email Services (NHS.Net) for use throughout the NHS, which is deemed suitable for the

transmission and receipt of patient and other confidential data. The use of personal email accounts for the transmission or receiving of patient or other person identifiable data is strictly forbidden and any individuals found doing so will be subject to disciplinary action.

6.3 All NHS Net accounts end with the suffix nhs.net. Sending and receiving information is allowed from and to other .nhs.net addresses e.g. joanne.bloggs@nhs.net. The Trust's email system ends with merseycare.nhs.uk and confidential information must not be sent to any other organisation unless the Trusts Email encryption solution is used. To encrypt a message type [secure] in the subject field of the email. For further information please contact the service desk.

6.4 The Trust Email system, falls within General Data Protection Regulations, and the Freedom of Information Act 2000 where emails stored identify living individuals, and as such may be subject to an access to personal data request.

6.5 All employees with access to Email will have responsibility for sending their own Emails. It is, therefore, imperative that the following guidance is read and understood:

6.6 All employees are prohibited in making (or forwarding) any derogatory remarks about any person or company by Email.

6.7 All employees must report any potentially defamatory material to their line manager as soon as it is identified so that steps can be taken to remove it permanently.

6.8 All employees are advised that even deleted items may not be eliminated permanently from the system and may be recovered if required.

6.9 All employees are advised not to send emails in anger or without thought and are prohibited from sending or forwarding any discriminatory messages even if intended as a joke.

6.10 Employees must be aware of the increased risk of confidential information being misdirected and thus the need to consider the use of a different medium in certain cases.

6.11 Employees must accept the risk that inbound Emails may contain explicit or offensive material that is beyond the control of the employer and the distribution of chain letters, inappropriate humour, explicit language or offensive images is not allowed on Trust resources. Employees must not use Email either internally or externally to harass anyone in any manner. Employees should avoid 'flame mail', where content is abusive towards other individuals, even in response to abuse being directed at them.

6.12 All email is automatically scanned for viruses and other malware when it comes into the Trust. However no measures can be 100% effective and there is still a small risk of such software arriving in a user's mailbox. If you are suspicious of the subject, source or authenticity of any received Email messages, you should not open the email and contact the Service Desk the earliest opportunity.

6.13 Employees have a responsibility to draft all Emails carefully, taking into account discrimination, harassment, company representation and defamation issues.

6.14 Email is an insecure system, and content can be easily copied, forwarded and archived. There is no guarantee that communications either internally or externally are private or that they will arrive at their destination at a particular

time or at all. Internet Email should not be utilised under any circumstances for the transmission of personal or confidential information.

6.15 Deletion of old emails is to be managed by each employee keeping in mind data storage levels, archival records, contractual evidence and legal discovery issues.

7 MONITORING INTERNET ACCESS AND EMAIL

7.1 All employees should be aware that to allow the business of the Trust to continue unhindered, or as part of an investigation, the Trust may require access to an individual's mailbox for example where an individual is away for a period and access is required for correspondence urgently. In such cases the Trust will, where possible, request access from the individual. Where this is not possible access will be granted by the IM&T Security Manager on receipt of a written request from a line director. When access is granted an email will be sent to the mailbox of the owner informing them that access has been granted and to whom. Access will be withdrawn as soon as the information required has been retrieved.

7.2 The Trust automatically tracks all Internet usage and in addition has an Internet content filtering system which blocks access to websites it deems inappropriate, or where the use of sites will impact on the business needs of the Trust. This system protects members of staff from accidentally accessing unsuitable websites, and will keep a detailed log of every page visited. The Internet content filtering system will block access to millions of sites however it cannot block every site deemed inappropriate. It is the user's responsibility not to access inappropriate sites; in addition the system may block sites that are required for legitimate business use. If this happens, users will need to contact the Service Desk to request the site to be permitted, authorisation from their manager citing the business need will also be required. The IT Security team will review the content and either approved or deny the requested access. If the Trust becomes aware that an employee (or group of employees) may be misusing their Internet access or email facility in contravention of this standard, steps will be taken immediately by the Line Manager/ IM&T Security Manager to suspend access, and to then consider what the appropriate level of intervention is going to be, with consideration being given to the options below;

a) Report the user to their line manager who will decide what further action will be taken.

b) Report the user to both the line Manager and HR who will decide what further action will need to be taken

c) Report the user to the police and assist them in carrying out a full investigation

7.3 For Option 1, IT Services staff will report to the employee's Line Manager and the Director of Human Resources only on material found on the computer, which contravenes this and any other relevant Trust Standard.

7.4 If the Line Manager, in conjunction with Human Resources, considers that this Standard has been breached, they will deal with the matter under the Trust's Disciplinary Procedure.

7.5 Any information discovered during the Trust's monitoring of email use and internet access will only be used to investigate a breach of this Standard and to pursue any subsequent necessary action, and should not be used for any other purpose. The standard process that will be followed can be found in the User Investigation Security Standard SS06

8 MONITORING AND COMPLIANCE OF THE STANDARD

8.1 This Standard will be reviewed and amended in accordance with any employment law, good practice guides and case law on an as and when required basis.

8.2 All emails are automatically scanned for viruses and Trojan code. All email traffic (incoming and outgoing) is logged automatically, and Users deletion at the desktop level does not remove emails from the system. These logs may be audited periodically and in some cases where agreed with HR and/or Senior Management, the message content itself might also be accessed for any proper business purpose including 'business as usual' or questions over 'inappropriate use' etc. The content of emails is not routinely monitored however the Trust reserves the right to monitor Email usage in accordance with, and subject to any changes of, legislation and/or Codes of Practice. This included the Regulation of Investigating Powers Act 2000 and the General Data Protection Regulations.

8.3 Internet access records are monitored electronically, and where site requests contradict electronic policy settings, then the user is notified and asked - on occasion - if they wish to override the exception.

8.4 If there is evidence that staff are not adhering to the guidelines set out in this Standard, the Trust reserves the right to question the individual member of staff, and to potentially take disciplinary action when deemed necessary, which may lead to summary dismissal and/or legal action.