NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON-CLINICAL DOCUMENT

Social Networking Security Standard

Standard Number:	SS01
Scope of this Document:	All Staff
Recommending Committee:	Joint Information Governance & Caldicott Committee
Approving Committee:	Joint Information Governance & Caldicot Committee
Date Ratified:	February 2020
Next Review Date (by):	December 2021
Version Number:	Version 3
Lead Executive Director:	Executive Director of Finance
Lead Author(s):	IM&T Security Manager

TRUST-WIDE NON-CLINICAL DOCUMENT

2020 – Version 3

Striving for perfect care and a just culture

TRUST-WIDE NON-CLINICAL DOCUMENT

SOCIAL NETWORKING SECURITY STANDARD

Further information about this document:

Document name	**Social Networking Security Standard SS01**
Document summary	**Trust Standard On the use of Social Networking**
Author(s) Contact(s) for further information about this document	**Mark Williams** **IM&T Security Manager** **Telephone: 0151 296 7643** **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 Policy 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
V3		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 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, sex, race, religion and belief (or lack thereof), sexual orientation, gender reassignment, pregnancy and maternity and marital and civil partnership status. The Equality Act also requires regard to socio-economic factors.

The trust is committed to promoting and advancing equality and removing and reducing discrimination and harassment and fostering good relations between people that hold a protected characteristic and those that do not 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 4
2 OUTCOME FOCUSED AIMS AND OBJECTIVES 4
3 ACCESS 4
4 SCOPE 5
4.1 Communication Staff 5
4.2 Staff 5

1 PURPOSE AND RATIONALE

1.1 **Purpose** – Social media/ networking is widespread in both personal and work environments. Examples of social media types/ sites include:

Facebook, Google+ and LinkedIn (social networking)
Twitter (micro-blogging)
YouTube and Instagram (Photo and video content sharing sites)
Blogs and personal websites
Messaging boards
Bookmarking websites

This list is not exhaustive as social media is a constantly evolving area and the types of social media available may change over time.

1.2 **Rationale** – Social networking in both a business and personal environment can have detrimental effects if not used correctly. This document outlines how the use of social networking should be carried out to safeguard the Trust.

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 Social networking on behalf of the trust is carried out safley and securley, representing the Trust in a professional manor

(b) To ensure that the Trusts Staff understand that the use of social networking can also have an effect on the organisation they are employed by.

(c) Ensure staff, understand their responsibilities when using social media and what should, and should not be electronically written or posted.

(d) Highlight potential risks for when staff post on a social networking site.

(e) Document Trust intentions for the use of social media.

(f) Ensure the Trust communicates the implications of using social media inappropriately.

(g) Ensure staff know where they can go for further advice.

3 ACCESS

3.1 Access to social media sites is restricted to view only with the exception of the communications department. If unrestricted access is required a request must be made to the service desk and approval from your service director will be required.

4 SCOPE

4.1 **Communication Staff** –The Trust uses social media as part of its Communication Strategy as the Communication Department has authority to speak on behalf of the Trust. It is responsible for managing the Trust official sites which include Facebook and Twitter.

Social media, like other communication tools, is used to improve the public's understanding of the Trust and its work, promote health, and engage with the general public.

When using social media sites, the Communication Department will, on behalf of the Trust, ensure it:

a) Is respectful towards patients, members of the public and Trust employees.

b) Does not reveal confidential or sensitive information about patients, staff or the Trust.

c) Updates the channels on a regular basis and respond to users posts.

d) Removes any content posted by other users that is considered offensive or derogatory.

e) Adheres to the IM & T Security policy.

4.2 **Staff** –When using Trust-owned computers, staff are allowed view-only access to Facebook and the ability to post on Twitter. When a member of staff identifies they work for the Trust and/ or discusses their work on any social networking site, they must behave professionally and in a way that respects confidentiality and protects patients, members of the public, work colleagues and the reputation of Mersey Care NHS Foundation Trust.

The standard sets out staff responsibilities when using social media and the legal implications involved. It is not intended to stop members of staff from using social media sites in their own time, but to outline some areas of best practice and illustrate where problems can arise for individual staff members and the Trust.

All staff have a responsibility to follow the principles with the use of social media and should ensure they read and follow the Trust policy on patient Confidentiality and Information Sharing (IT10) in order to avoid facing disciplinary action in line with the Service disciplinary policy (HR01).

Social media has blurred the boundary between the private and professional lives of staff and staff that use social media in their personal life should be mindful that inappropriate use could damage their own reputation and that of the Trust.

When a member of staff identifies their association with the Trust by, for example, stating they work for Mersey Care NHS Trust, posting pictures of them in uniform and/ or discusses their work, they are expected to behave professionally and in a way that is consistent with the Trust values and policies. Even if a staff member does not directly associate themselves with the Trust, their link with the organisation can become known through images on the sites of their friends, on the Trust website or by and internet search using a search engine.

When using any social media channel staff should follow the principles outlined below:

a) Staff may use personal social media sites during their working hours in agreement with the time agreed by their Line Manager.

b) Use of personal devices to access social media sites should be limited to allocated break times.

c) If a member of staff discloses that they work for the Trust or can be identified as an employee through association with other people, they should ensure their profile and related content is consistent with how the Trust would expect them to present themselves to colleagues and business contacts.

d) Staff should make it clear that their views are their own, not those of their employer.

e) As all official social media sites are managed by the Communication Department, no other teams/ staff within the Trust should set up corporate sites without the authorisation of the Communication Department.

f) Staff should not set up sites that are made to resemble an official site.

g) If a member of staff associates themselves with Mersey Care NHS Foundation Trust on their social media site, they are expected to post under their real name to demonstrate openness, honesty and accountability.

h) If an employee posts under a pseudonym and at a later stage these posts are associated with their real name, all previous posts will be admissible in a disciplinary investigation or hearing.

i) Posts must not contain anything contrary to the Trusts equality and inclusion policy. Anything containing racist, sexist, homophobic, sexually explicit, threatening, abusive, disrespectful or other unlawful comments must not be published.

j) Staff should seek permission from colleagues before posting personal details or images that may link them with the Trust and should not post anything about someone if they have been asked not to. Staff must always remove information about a colleague if they have been asked to do so.

k) Staff should be aware of privacy limitations when posting material using social media, and the extent to which information can be in the public domain.

l) Whatever is posted on a social media site could be in the public domain immediately or, if initially shared with a limited group of followers or friends, could still be copied and shared or published elsewhere.

m) Staff should carefully consider what they want to say before they publish anything, and work on the basis that anything they write or post could be shared more widely without their knowledge or permission.

n) Staff should be careful when sharing or retweeting posts, as they could be seen to be endorsing someone else's point of view.

o) Staff must ensure the information they posts is factually correct. If they discover they have reported something incorrectly, they should amend it and make it clear they have done so.

p) All comments must be legal and must not incite people to commit a crime.

q) Staff could face legal proceedings for posted comments aimed at named individuals or an organisation that are considered to harm reputation(s).

r) Staff must not use the Trust crest or the NHS logo anywhere on their social media sites, or copy photos from the Trust internet or intranet sites – these are copyright protected.

s) Staff should only share information about the Trust that is in the public domain, and should not add derogatory comments on these issues.

t) Staff must also respect patient confidentiality, and should not disclose information that could identify a patient.

u) Staff should not air grievances or publish anything that risks bringing the Trust into disrepute.

v) If staff post any photos of themselves or colleagues in uniform, or in an identifiable work setting, they must ensure that these represent a professional image of the Trust. Staff should not use a photo of themselves in uniform as their profile picture; this could give the impression that their site is an official site.

w) Staff must not post images containing patients on personal social media accounts. They should also not post images of any incidents they have attended. This does not prevent staff sharing, retweeting or linking to images that have been published on official Service sites.

In addition, staff should configure their privacy settings and review them regularly as:

a) Social media sites cannot guarantee confidentiality and are able to change their settings without prior notification.
b) The public, employers or any organisation staff have a relationship with may be able to access their personal information.

c) Once information is online, it can be difficult to remove it.

Confidentiality must be respected by anyone who posts anything about their work on the internet, and under no circumstances should anything be posted that identifies a patient.

Staff should ensure they know Trust's policy on patient confidentiality and follow it at all times.

The Department of Health (DoH) guidance on patient confidentiality is contained in the publication 'Confidentiality: NHS Code of Practice (Nov 2003)'. It states that all NHS staff have a duty to keep all information about patients confidential and to not disclose this information to anyone not involved directly in their care. It is a legal obligation derived from case law, a requirement within professional codes of conduct and is included in NHS employment contracts as a specific requirement linked to disciplinary procedures.

It is generally accepted that information provided by patients to the health service is provided in confidence and must be treated as such so long as it remains capable of identifying the individual it relates to. Once information is effectively anonymised it is no longer confidential.

Whilst there are no clear obligations of confidentiality that apply to the deceased, the DoH and the General Medical Council agree there is an ethical basis for requiring that confidentiality obligations must continue to apply.

It is against trust policy to disclose Identifiable information to the media or for publicity purposes. As well as names and other personal details, this includes the use of images of the patient undergoing treatment in a real life situation and where the patient is posing for a picture.

The following is patient-identifiable information and should not be disclosed:

a) Name, address, full postcode or date of birth.

b) Pictures, photographs, videos, audio-tapes or other images.

c) NHS number and local patient identifiable codes.

4.3 Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

4.4 The DoH definition of anonymised information is "information which does not identify a patient directly, and which cannot reasonably be used to determine identity". Anonymisation requires the removal of name, address, full postcode and any other detail or combinations of details that might support identification."