Western Health and Social Care Trust

Social Media Policy

November 2023

Policy Title	**Social Media Policy**
Policy Reference Number	**Corp13/002**
Implementation Date	**March 2023**
Review Date	**March 2028**
Responsible Officer	**Oliver Kelly, Head of Communications**

Contents		

1.0 Introduction

Social media is a form of digital marketing and communication that is direct, personal, instant and responsive. It provides us with many cost effective opportunities to improve the way we communicate, reach out and interact with different communities we serve. Social media, when used appropriately, can support the business objectives of the organisation and help the Trust to better connect with the public, patients, clients and other regional groups with the general public/target people.

Social media refers to internet and mobile-based tools used for the generation, dissemination and discussion of information in textual, pictorial, audio, video formats. Under this policy, social media includes all forms of current and future tools used for digital social interactions between people.

Over half of the population in Northern Ireland engage in social media. As of January 2022, 63% of the population of Ireland have a Facebook account, 48% have an Instagram account, 31% have a LinkedIn profile and 25% have a Twitter account.

Social media may include (but is not limited to):

- Social networking sites (Facebook, Instagram, LinkedIn);
- Video and photo sharing websites (YouTube, Vimeo);
- Mobile Messaging Apps (WhatsApp, Facebook Messenger);
- Personal and corporate blogs;
- Micro-blogging (Twitter);
- Wikis and online collaborations;
- Forums, discussions boards, groups.

Whilst employees are restricted to access on such sites via a Western Trust networked computer at present, many employees use social networking sites during personal / leisure times and often through personal mobile phones.

Access to social networking sites, from Trust networked computers, is controlled within the Trust by “Group policies”. This would enable certain users or staff to access social media sites.

Guest (WiFi) Network does not have the same restrictions or limitations as the Trust network. Guest access is available in all Acute and a large proportion of Trust community sites. This enables patients, clients, visitors and staff to use their own personal devices (e.g. smartphones, laptops) to connect to the internet and thereby social media sites.

Those staff using Trust mobile phones with internet capability can connect to the Guest (WiFi) Network, where available, and access social media sites. Alternatively, any Trust phone with a data contract and a 4G connection can access social media sites at any time or anywhere (assuming there is connectivity).

Guidance is required to ensure employees do not act in a way that may negatively affect the reputation of the Trust, and to ensure employees do not compromise their professional code of conduct and / or conditions of contract of employment by discussing work-related issues.

2.0 Purpose

The purpose of this social media policy is to guide and protect Trust reputation and set standards for employees. This is to ensure consistency across channels when staff are engaging in social media in a personal or professional context.

This policy sets out the principles which employees of the Western Trust are expected to follow when using social media in their personal and professional lives. The intention of this policy is not to stop Trust employees from conducting legitimate activities on the internet, but rather serves to provide guidance to employees to engage on social media platforms. Employees can feel empowered to enhance creativity and show their personalities without having to be concerned that the content they are sharing on social media would negatively impact on their career.

Individuals can often feel less inhibited when posting comments online and as a result say things they would not express in other circumstances. Posting comments under a username does not guarantee anonymity as any comments made online can be traced back to the author.

As a rule, staff should never share or post personal information belonging to patients, clients or staff or post business sensitive information, on any social media platform.

3.0 Objectives of the policy

This policy has the following objectives for Western Trust employees:

- To ensure safe, professional use of social media tools.
- To make employees aware of the issues relating to the use of social media for both private and professional purposes, and be aware of their responsibility as an employee of the Trust.
- To ensure employees are aware of all relevant legislation and standards relating to online information, including codes of practice from related professional bodies.
- To enable the Corporate Communications Department to actively manage Western Trust corporate social media channels in a safe environment and to monitor social media channels.

4.0 Compliance with related legislation, policies and guidance

This policy supports the Western Trust Data Protection and Confidentiality Policy (2021); Disciplinary Policy & Procedure (2022) and the Regional / Local Digital Policies, Technical and User standards.
This document should also be read in association with relevant policies and legislation. This includes, but may not be limited to, the following professional policy and guidance documents and legislation:

- https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentiality-service-user-information
- Guidance on the recording of staff by service users
- Social Media, Ethics and Professionalism Guidance [BMA 2018]
- Doctors Use of Social Media [General Medical Council 2013]
- Social Networking Guidance [Northern Ireland Social Care Council]
- Social Media Guidance [Nursing and Midwifery Council]
- Defamation Act (Northern Ireland (2022): Defamation law can apply to any comments posted on the web, irrespective of whether they are made in a personal or professional capacity. Defamation is the act of making an unjustified statement about a person or organisation that is considered to harm their reputation. If an individual makes a statement that is alleged to be defamatory, it could result in legal action against the individual and the organisation they are representing.
- Protection from Harassment (Northern Ireland) Order (1997): In order to show harassment a victim will have to demonstrate the alleged individual is causing harassment, alarm or distress by using threatening, abusive or insulting words or behaviour.
- Data Protection Legislation (UK GDPR and Data Protection Act 2018)
- Computer Misuse Act 1990
- Human Rights Act 1998

This policy also supports the Western Trust Employment Contract which states:

10. Through the course of your employment you may become aware of information concerning patients or staff. All such information must be treated as confidential and you are required to comply with the requirements of the Data Protection Act 2018, the General Data Protection Regulation and associated legislation and regulations. It should be noted that any unauthorised disclosure of information covered by data protection legislation is a criminal offence for which you will be held personally liable in law.

Any breach of this confidence in any format, including for example via Social Networking sites (which include but are not restricted to Facebook, Twitter and

messaging services) will result in action being taken under the Disciplinary Procedure and may lead to dismissal.

On termination of employment with the Trust, you should not disclose any information or matter to which you had access during your employment. Should you do so the Trust reserves the right to take any action considered appropriate in the circumstances.

11. Your personal data will be held by the Trust on manual and computer records and will be processed in accordance with Data Protection legislation. Further information is available from the Human Resources Department. You are also advised that you have a statutory obligation under Data Protection principles to protect any personal data to which you have access in the course of your employment. Any employee who unlawfully discloses personal data may be subject to disciplinary action by the Trust. You should also be aware that regardless of any action by the Trust, unauthorised disclosure

5.0 Policy scope

- This policy applies to the use of all social media (outlined in 1.0) for both professional and personal purposes.
- This policy applies to all employees on a Trust contract, including those on temporary, student, honorary and any agency workers engaged by the Trust.
- This policy applies regardless of whether the social media sites are accessed using Trust ICT facilities and equipment or personal equipment belonging to employees.

6.0 Policy statement

6.1 Personal use

As Trust employees it is important to be aware that if you post information or views about the Trust, or connected to your employment with the Trust, during personal time they cannot be isolated from your working life. You should assume that all comments, likes and shares you make are in the public domain and could potentially remain so forever. Also, if you have posted, liked or shared posts anonymously, at some point your identity and nature of employment could be revealed.

Comments about the Trust, patients, clients, colleagues or members of the public can bring the Trust into disrepute and may result in the Trust or respective employees being liable to legal action. Liking, sharing and commenting on content shared on social media by other users that goes against the Trust's values can be

publicly seen by others and may also result in the Trust or respective employees being liable to legal action. It is imperative that confidentiality must be maintained at all times.

The following policy statement is designed to protect the Trust and the employee from risk of allegation, disrepute or liability:

Employees should:

6.1.1 never include any work related information on any social media sites. Work-related conversations that would be inappropriate on a bus for example, are just as inappropriate on a social networking site.

6.1.2 never share confidential information online, for example, identifiable personal information about patients, clients or other employees, or confidential Trust business

6.1.3 never post inappropriate comments about employees, patients, clients or members of the public.[1]

6.1.4 never like, share, react to or comment on posts shared by others on social media where the content goes against the values of the Trust

6.1.5 never post or take photographs on Western Trust premises, pictures of patients or service users, without prior agreement from the Communication Team where agreement to take photographs and the use of the images will be explicitly discussed with patients / service users and written or verbal consent gained. Employees should refrain from posting photos of work colleagues on work related social events, or in work related uniforms online. Some colleagues will object to their photographs being on websites and this can cause offence.

6.1.6 never post video/audio and sound clips recorded in the workplace for non-professional means.

6.1.7 never use social media sites to bully or intimidate another member of staff or members of the public (including posting inappropriate or offensive comments and pictures).

6.1.8 never use social media sites in any way which is unlawful.

6.1.9 refrain from accepting a 'friend request' from a patient or client (or their family member) that you only know through professional work / contact,.

[1] [For more advice about staying safe on social networking sites visit the Information Commissioner's Office website]

6.1.10 remove yourself if you have previously accepted a friend request from a patient, client or their family members, who you only know through professional work.

6.1.11 monitor and remove content shared within social media groups and pages, where the content goes against the values of the Trust, and where the staff member is an admin of the group or page.

6.1.12 never impart any information that could be considered sensitive, such as third party supplied details.

6.1.13 notify the Communications Team if they are contacted by media or public representatives via their personal social media.

6.1.14 Western Trust internet security software may block use of social networking sites. Employees must not attempt to access social networking sites from any Trust PC / laptop / mobile phone or any other electronic device.

6.1.15 not access social media sites during work hours via personal smart phones (with the exception of allocated break times).

This list is kept under review by the Corporate Communications Department and additions will only be added once jointly approved by Information Governance, ICT Services and Human Resources. The Trust recommends that employees using social media sites for personal recreation do not mention their work or any related activities.

6. 2 Professional Use

If an employee identifies themselves as a Western Trust employee on a social media website they will ensure their profile and related content is consistent with how they would present themselves with a patient / client or whilst in a work setting.

Employees should never use any religious, racial, sexual, political or any other references or images that may cause offence when using social media.

If you are writing in a professional capacity, you should identify yourself. Any material written by authors who represent themselves as doctors or a medical professional are likely to be taken on trust and/or to represent the views of the profession more widely. You should also be aware that content uploaded anonymously can, in many cases, be traced back to its point of origin.

If you are concerned about a colleagues' behaviour online, you should take steps to raise your concern with their line manager. Also, if staff are aware of online content that could harm the reputation of the Trust or any member of employees or service

user, it must to be reported immediately to their line manager, who will report this to the Trust's Communications Team and HR Department for action or disciplinary advice.

If employees publish information on the internet relating to work or services associated with the Western Trust, use a disclaimer such as "The views expressed are my own and do not necessarily represent the views of the Western Trust."

Employees should maintain boundaries between their personal and professional lives by customising their privacy settings for social media websites and avoiding personal information becoming visible.

Employees are wholly responsible for any content they decided to post or share.

Western Trust employees must not use mobile messaging apps including WhatsApp or Facebook Messenger to discuss or share patient/client information. These apps are only to be used in a professional setting based on the guidance/ approval from the Trust ICT and Information Governance Departments following a Data Protection Impact Assessment.

A Social Media Guidance for Staff Video is available to provide guidelines and to help staff "think before you post". Video is available here.

6.3 Dealing with Negativity

Where staff find a malicious or abusive post on social media, they should avoid responding directly as this may make the situation more difficult. Staff are advised to take screenshots of malicious or abusive posts, as repeated posts of a similar nature may constitute harassment. Staff are also reminded that they can block accounts posting malicious or abusive content. Where staff health and wellbeing are impacted as a result, they should seek advice from their line manager and notify the Corporate Communications Team.

6.4 Recordings of staff by a service user – Overt/Covert

Although we cannot place restrictions on a service user wishing to record notes of a consultation, care or conversation with a health professional, staff should act in a professional manner at all times. Staff should aim to facilitate a request to record in these circumstances. Where organisations are aware that covert recording is a significant issue they should aim to discourage service users from doing so.

See Guidance on the Recording of Staff by Service Users within Health and Social Care

6.5 Corporate Use

The Western Trust Communications Department creates, maintains and operates ALL Trust corporate social media channels to engage with key stakeholders, thus protecting all relevant security and passwords for such accounts.

Western Trust corporate social media accounts will be regularly monitored. The Communications Department will regularly review the Trust's channels and monitor other social media for references to Western Trust business during normal working hours and will share this information internally with relevant employees. Where inappropriate comments on Western Trust social media channels are brought to the attention of the Communications Department, immediate action will be taken in accordance with moderation clauses listed below (point 6.3.1).

The Communications Department will only use images of patients / clients in social media where informed consent has been given verbally or in writing by completing and signing an official photography consent form. Consent from a parent or guardian must be given for anyone under the age of 16 years old.

The Western Trust does NOT permit the setting up of social media accounts for individual Trust services. The Communications Department will monitor and remove when necessary any social media profiles that have been set up using departmental imagery/content without permission. The creation of social media accounts for ALL Trust purposes are at the discretion of the Communications Team. Staff who wish to promote their services on social media must do via the corporate Western Trust social media channels. For support in promoting services on Western Trust social media channels, staff should contact the Communications Team.

All feedback to the Western Trust received through social media channels will be sent to the relevant service area and should be considered by employees prior to developing an appropriate response with support from the Communications Department.

Responses to public posts may be conversational, objective, and polite in tone with information sharing the main goal and will require Assistant Director approval.

6.5.1 Moderation / Unacceptable content: Certain types of content will be removed from our social media channel on the following grounds. The Western Trust reserves the right to ignore/remove comments without notification, including those which:

- bully, harass or intimidate any individual or organisation
- are unlawful, libellous, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive

- are deceptive or misleading
- infringe or violate someone else's rights
- violate the law
- violate any intellectual property rights
- discuss ongoing legal proceedings
- are spam
- advertise products or services
- are irrelevant or off-topic
- are disruptive
- are repetitive
- may impact upon the Trusts' reputation.

We will also remove, ban, block or report any user who:

- continues to post comments such as those listed above
- encourages others to post such comments
- uses offensive images as their profile picture
- has user name which may be considered as offensive.

The Western Trust will only have control over comments on our own corporate channels, however, the Corporate Communications Department will alert employees and services to comments on other sites if required.

Western Trust social media channels will not be used to deal with urgent or media enquiries or queries from staff although we reserve the right to comment on inaccurate coverage or insightful comments.

We reserve the right to modify or change these conditions at any time.

7.0 Roles and responsibilities

The following groups are responsible for the adoption of the policy:

- All employees are responsible for the implementation of this policy in line with their role within the organisation.
- Any misuse of social media should be reported to your line manager or agency. It is the responsibility of the line manager to investigate any reported breaches of this policy in conjunction with Human Resources, Information Governance, Communications and ICT Services.
- The Communications Team will have the primary responsibility for monitoring the Western Trust's corporate use of Social Media in conjunction with Information Governance and ICT. The Communications Team will develop a communications action plan to profile this policy with staff. The Communications Team will be available to provide presentations about this policy and corporate use of social media to teams on request.

8.0 Breach of Policy

Non-compliance with this policy will be dealt with under the Trust's Disciplinary Procedure and referral to a professional body as appropriate.

Investigation under the Trust's Disciplinary Procedure may result in a range of actions being taken, such as an informal warning being issued. More serious breaches will be considered by a disciplinary panel and depending on the nature of the misdemeanour sanctions range from a formal warning to dismissal from your employment.

9.0 Review

This policy will be monitored and reviewed at regular intervals in consultation with the recognised trade unions collectively and not later than August 2028.

This policy has been screened for equality and human rights implications. No equality issues have been identified and it has been identified that a full EQIA is not required.