****

**IT Acceptable Use and Social Media Policy**

**[Date of Issue]**

|  |  |
| --- | --- |
| Policy Lead: | [Policy Lead] |
| Version No. | 1 |
| Date of Issue: | [Date of Issue] |
| Date for Review: | [Date of Review] |

CONTENTS

[1. Introduction 3](#_Toc148007938)

[2. Policy Statement 3](#_Toc148007939)

[3. Scope 3](#_Toc148007940)

[4. Definitions 4](#_Toc148007941)

[5. Business Use of Social Media 5](#_Toc148007942)

[6. Key Principles 5](#_Toc148007943)

[7. Confidentiality 6](#_Toc148007944)

[8. Professional Boundaries 7](#_Toc148007945)

[9. Personal Privacy 7](#_Toc148007946)

[10. Personal Use of Social Media 7](#_Toc148007947)

[11. Bullying and Harassment 8](#_Toc148007948)

[12. Raising a Concern 8](#_Toc148007949)

[13. Use of Email 9](#_Toc148007950)

[14. Use of Internet 11](#_Toc148007951)

[15. Roles and Responsibilities 12](#_Toc148007952)

[16. Monitoring 12](#_Toc148007953)

[17. Related Policies 12](#_Toc148007954)

[18. Legislation and Guidance 13](#_Toc148007955)

[19. Summary of Review 14](#_Toc148007956)

**[DELETE AS APPROPRIATE] [Company Name] does not currently operate on any social media platforms other than their private website. However, they may choose to do so in the future so social media use is incorporated into this policy**

# Introduction

The use of the internet and social media has become an integral part of everyday life. [Company Name] must embrace this for its opportunities, but also carefully manage its use to ensure appropriate protection for all users.

Used well, the internet and social media can improve the way information is shared, empowering clients and staff and improving openness and transparency. [Company Name] has an obligation to ensure those using the internet and social media while working at or for the Company, or in relation to Company activities are absolutely clear of the expectations regarding professional behaviour, protecting client confidentiality and safeguarding.

The social media ethos is all about engagement, participation and relationship building. Every platform encourages its users to take part by commenting on what they see and getting involved in conversations with others. This makes it a particularly useful vehicle both for informing clients and for gaining their feedback. Used well, social media can be part of collaborative working and co-production.

# Policy Statement

This policy sets out [Company Name]’s expectations for internet and social media use for individuals working within or on behalf of the Company.

# Scope

This policy and its procedures apply to all individuals working within or on behalf of [Company Name].

The scope of this policy includes use of both [Company Name] and personal resources to access the internet, email and social media, including outside of working hours. All individuals are expected to maintain a professional approach to work, clients and colleagues at all times and must not bring [Company Name]’s name into disrepute.

Social media is rapidly evolving and expanding so this policy will focus mainly on the most popular and commonplace social media platforms currently available:

* Microblogging (e.g., Twitter)
* Blogging (e.g., WordPress and Tumblr)
* Social sharing (e.g., Facebook)
* Video sharing (e.g., YouTube, Vimeo and TikTok)
* Picture sharing (e.g., Flickr, Instagram and Pinterest)
* Professional sharing (e.g., LinkedIn)
* Social bookmarking (e.g., Reddit, Scoop.it, StumbleUpon and Delicious).

# Definitions

**Social media** - the generic term given to any form of internet-based platform which enables online interaction and communication between users. Social media can include text, audio, video, images, podcasts and other multimedia communications.

**Social networking** - the use of social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life.

**Microblogging** - the practice of posting short messages or digital content (essentially this is blogging with a very limited word count). Twitter is an example of a microblogging site as it limits messages (or “tweets”) to 280 characters in length.

**Blogging** - the use of a public website to write an on-line diary (known as a blog), sharing thoughts and opinions on various subjects.

**Social sharing** - a form of social networking website that allows registered users to create personal profiles, upload photos and videos, send messages and keep in touch.

**Video/picture sharing** - allows anyone to upload short videos or pictures to a website either for restricted viewing (to a limited list of friends or viewers) or as a showcase to the wider public.

**Professional sharing** - a form of social networking website that is geared towards companies and industry professionals looking to make new business contacts or keep in touch with previous co-workers, affiliates and clients. Members can create customisable profiles that detail employment history, business accomplishments and other professional accolades.

# Business Use of Social Media

**[DELETE AS APPROPRIATE] [Company Name] does not currently operate on any social media platforms other than their private website. However, they may choose to do so in the future so social media use is incorporated into this policy**

[Company Name] maintains its own corporate presence on the following social media channels **[Delete as applicable]**:

* Facebook
* Instagram
* In direct response to patient feedback on public websites
* YouTube
* LinkedIn

Maintaining an active presence on social media sites allows [Company Name] to effectively manage its corporate brand and communication to stakeholders online. It is also an important way to be open and engage with the people we serve. This is overseen by the Registered Manager. Content deemed suitable for corporate social media includes:

* News, events and activities that are related to [Company Name]’s business.
* Content that provides a direct link back to [Company Name]’s external website.
* New developments, awards or achievements in [Company Name].
* Engagement with people who have an interest in [Company Name].
* Information that enhances [Company Name]’s reputation.

All social media accounts associated with [Company Name]’s business and activities are expected to adhere to the principles and expectations of this policy. [Company Name] will take all steps available to close down any linked social media account found to be acting outside of this policy.

# Key Principles

These key principles apply to all individuals working with [Company Name] who use email, internet or make use of social media, whether personal or professional, using Company or personal equipment, inside or outside working hours.

The intention of these principles is not to prevent staff from conducting legitimate activities on the internet in their personal time, nor to stifle constructive feedback, but serves to highlight those areas in which problems are most likely to arise for both individual staff members and [Company Name].

# Confidentiality

All staff have a responsibility to maintain and protect client, colleague and company confidentiality. Under no circumstances should they identify clients, or post information that may lead to the identification of the individual or post information that is stigmatising or derogatory to any client group or condition. This includes never disclosing information which may be:

* sensitive
* confidential
* subject to a non-disclosure agreement.

Staff using social media for work purposes can be only held liable for a breach under the Data Protection Act 2018, if the breach is wilful, otherwise [Company Name] is liable as Data Controller.

If staff do disclose any such information, then they are interfering with privacy and breaching the law on confidentiality, their employment contract and their professional Code of Practice (where applicable).

When creating a new corporate social media account, a data protection impact assessment should be completed to ensure that information governance standards are adhered to. The DPIA will form part of the guidance and support provided to staff using social media channels. Further information can be found in the Information Governance Policy.

**Staff are a representative of the business**

Staff should never post a comment, photo or video online that they would not be willing to share with people in “real” life in a face-to-face setting.

Online behaviour not only reflects on the staff members, but also on [Company Name] and the profession. While there is often a focus on the negative impact of social media on an organisation and its reputation, staff must remember that they have the potential to act as a positive and respected ambassador for [Company Name].

Everything that is posted online, including photographs, is public: even with the strictest privacy settings. Once something is online, it can be copied and redistributed, and it is easy to lose control of it. Staff should presume that everything they post online will be permanent and will be shared. They should refrain from any action or activity which may bring negativity upon them, their colleagues, their profession or [Company Name]. This may include posting on any social media (whether text, images, video or audio) defamatory, derogatory or offensive comments or attitudes (whether explicit or implied) towards:

* clients, their relatives, carers or visitors
* colleagues, direct reports or managers
* [Company Name] or its contractors.

# Professional Boundaries

Staff must not use social media to build or pursue relationships with clients, their families or carers, even if they are no longer in their care. If a friendship request from a current or former client or their relative is received, some sites, such as Facebook, allow for request to be ignored without the person being informed, avoiding unnecessary offence.

# Personal Privacy

Staff should think carefully about what kind of information they want to share and with whom and adjust their privacy settings accordingly. For example, on Facebook, privacy settings can be adjusted at group level to share different levels of information with different groups of friends. Staff should remember that the more their personal life is exposed through social media, the more likely it is that this could have a negative impact on them, their reputation and that of [Company Name].

# Personal Use of Social Media

Personal use of social media should be restricted to agreed rest/lunch breaks and should comply with the principles in this policy. The principles exist to protect everyone using the internet and social media. Professional use via a personal account, such as at a conference or other work-related event, is acceptable during working hours.

[Company Name] acknowledges that social media provides a number of benefits in which staff may wish to participate. Whether or not a staff member explicitly declares their association with [Company Name] on social media, they are expected to behave appropriately and professionally at all times, and in a manner which is consistent with the policies of the business, as well as the relevant professional codes of conduct.

[Company Name] and individual professional bodies have issued specific guidance to their members in relation to the use of social media:

* Royal College of Nursing (RCN)
* Health and Care Professions Council (HCPC)

Staff holding professional registration should be aware of their responsibility to uphold the reputation of their profession, and that their conduct online could jeopardise their registration if their fitness to practice is called into question.

Staff who are found to breach this policy may be subject to disciplinary action in line with the Disciplinary Policy.

# Bullying and Harassment

The use or social networking or blogging sites to bully, harass or intimidate other individuals within [Company Name] will lead to investigation and may result in disciplinary action being taken. More information is available in the Bullying and Harassment Policy. Staff who have concerns about this should contact the Registered Manager with a copy of the content.

Staff can also take action themselves to block a contact or remove someone from a friends list. Staff can also report inappropriate use of a site using the processes made available on most reputable sites. In the most serious circumstances, for example if someone's use of a social networking site is unlawful, the incident should be reported to the police.

# Raising a Concern

Individuals who become aware of a breach of this policy have a duty to report it to the Registered Manager.

Once made aware of a breach in the policy, the Registered Manager should seek Human Resources (HR) advice and where possible resolve the matter informally and locally. Where it concerns clients, the Safeguarding Lead should be notified and where possible the matter should be resolved informally and locally.

If a staff member feels that they are the target of complaints or abuse on social media sites, they can remove someone from their friends or followers list and block them from interacting. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others. If staff have reason to believe that the activity is originating from a colleague or client, they should alert the Registered Manager.

Any grievance with [Company Name] should be channelled through procedures and policies already in place and dealt with in the work environment. They should **not** be displayed or discussed via social media.

# Use of Email

[Company Name] provides an email service primarily for business purposes.

All [Company Name] business must be carried using out on [Company Name]’s email accounts where available, and not using consumer internet-based email services (e.g., Gmail or Yahoo). Although [Company Name]’s email is provided primarily for business use, responsible reasonable personal use is permitted, provided all use is outside of normal working hours and:

* does not contravene any of [Company Name]’s policies and guidelines
* is not detrimental to [Company Name]’s image
* is not for personal gain
* does not constitute a solicitation or harassment
* does not interfere with work
* it is indicated, where appropriate, that the view expressed is solely a personal view and not that of [Company Name]
* is not illegal.

The personal use of the email account provided by [Company Name] may create the impression that a staff member represents the organisation. As such, if they wish to engage in promotion or discussions of personal, political, financial, commercial, social or religious views, this should not be performed in work time nor with the Company’s e-mail account. In all such instances staff should also avoid commenting on any of [Company Name]’s policies, issues or products.

The following practices are strictly prohibited and may be subject to disciplinary action, up to and including dismissal:

* sending unsolicited junk email, “for profit messages” or chain letters
* attempts at sending harassing, obscene, offensive and/or other threatening email
* attempts to read, delete, copy, modify, or send email on behalf of other workers without prior permission
* attempts to intercept other workers’ email
* forgery (or attempted forgery) of email messages
* unreasonable use of email for personal use.

Staff must not use e-mail either internally or externally to harass anyone, (known as “cyber bullying”,) where content is abusive towards other individuals even in response to abuse being directed at them.

Staff should, wherever possible, adopt the following good practices when managing all emails:

* ensure that emails are checked regularly, at least every 2 working days
* make use of the ‘out of office’ function when on annual leave or sick leave
* avoid overusing email by thinking carefully about who emails are sent to and avoiding unnecessary courtesy copies (cc’s of emails)
* carefully use the “Reply All” feature
* do not reply to an email simply to inform the sender that you have received it
* use care and judgment when composing emails (email is a written record that can be distributed onwards freely and should not be treated as a “conversation”)
* when replying to email, it is often useful to include the relevant portion of the originator’s email to put your reply into context but delete unimportant portions of the original message to prevent the message from getting too long.

If staff are unsure about the material they wish to send or are concerned about any material which they may have received, they must discuss this with the Registered Manager. Issues of confidentiality, copyright and data/information protection must be discussed with the Data Protection Officer/Data Protection Lead/Registered Manager.

Person Identifiable Information sent to external email addresses must be encrypted or password protected where appropriate.

Upon notification of a staff member leaving the Company, their email account must be deactivated with immediate effect. It is the responsibility of the Registered Manager to ensure that any information required is transferred prior to the staff member’s departure from the Company.

# Use of Internet

The internet service is predominantly available for matters relating to the business of [Company Name]. [Company Name] accepts that there will be occasions when workers need to access internet services for personal use. This should be used with discretion and all users are expected to act responsibly and access this facility preferably in their own time and out of working hours. It is also important to give thought to the impact of internet use on business systems (for example large downloads, or streaming video).

[Company Name]’s corporate internet service allows worker access to the internet through the corporate network from his/her [Company Name] PC, laptop, iPhone, or tablet. No other method of accessing the internet (e.g., via a broadband connection using a separate Internet Service Provider) is permitted without requesting authorisation from the IT team/Registered Manager.

Users must not alter the configuration of the internet security settings on their PCs. Users must not load any software onto their PCs without prior consultation with the IT team/Registered Manager.

The following practices are strictly prohibited and may be subject to disciplinary action, up to and including dismissal.

* online gambling
* downloading, printing, creating or distributing pornographic or any other material of a sexual nature
* engaging in criminal activities
* downloading, printing, creating or distributing offensive or harassment material with regard to race, gender, ethnic origin, sexual orientation, age, disability, religious or political beliefs
* carrying out a private business
* downloading or distributing pirated data or software
* knowingly disabling or overloading the network
* knowingly circumventing any system intended to protect the privacy and/or security of the organisation or another user.

[Company Name] will make every reasonable attempt to ensure it is not possible to access inappropriate content (e.g., pornographic material), and may block access to certain websites. With the exponential growth of the internet, some sites may not have been added to the current list of blocked sites.

Categories of sites that have been blocked are available from the Registered Manager. If you believe a website should be blocked or if a site you need to use has been inadvertently blocked, please contact the Registered Manager for assistance.

# Roles and Responsibilities

The Registered Manager is responsible for:

* ensuring that staff know how to access current [Company Name] policies and that where these are not being adhered to, discuss the standards and expectations required with the staff member concerned
* understanding the policy and how to escalate concerns that cannot be locally resolved.

All individuals who work with [Company Name]are responsible for:

* reporting inappropriate use as outlined in this policy to the Registered Manager in the first instance or to another staff member.

# Monitoring

Compliance with this policy will be monitored by the Registered Manager through routine audits of Company and personal media, as well as any feedback from clients and/or staff.

# Related Policies

* Bullying and Harassment Policy
* Confidentiality Policy
* Disciplinary Policy
* Grievance Policy
* Information Governance and Record Keeping Policy
* Whistleblowing Policy

# Legislation and Guidance

**Relevant Legislation**

* Data Protection Act 2018

**Guidance**

* [Read Social media guidance online (nmc.org.uk)](https://www.nmc.org.uk/standards/guidance/social-media-guidance/read-social-media-guidance-online/)
* [Communication and using social media | (hcpc-uk.org)](https://www.hcpc-uk.org/standards/meeting-our-standards/communication-and-using-social-media/)

# Summary of Review

|  |  |
| --- | --- |
| Version | 1 |
| Last amended | [Date of Issue] |
| Reason for Review |  |
| Were changes made? |  |
| Summary of changes |  |
| Target audience | Care staff, Managers |
| Next Review Date | [Date of Review] |