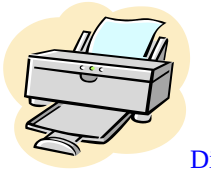
CC_IG31 INTERNET AND SOCIAL MEDIA USE POLICY FOR STAFF, PATIENTS AND VISITORS

Document name:	Internet and Social Media Use Policy for Staff, Patients and Visitors
Document Classification:	Corporate - IG
Document No:	IG31
Version:	1.1
Name of originator/author:	Anna Bernard
Policy Owner:	HR Director
Date created	09/12/2015
Date ratified:	Dec 2015
Date reviewed	26/09/2019
Ratified by:	HR Director
Responsible committee:	Exec Board
Superseded policy (if applicable):	CC_HR17_Social Media Policyv1.1
Next review date:	Sep 2022
Target audience:	Directors, Managers, Clinicians, Staff



Contents

1. *Introduction*

The use of the internet and social media has become an integral part of everyday life. The NHS 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 we share information, can empower patients and staff and can improve the openness and transparency of NHS organisations. We have an obligation to ensure those using the internet and social media at clinic locations, or in relation to Organisational activity, are absolutely clear about our expectations regarding professional behaviour, protecting patient 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 patients and for gaining their feedback. Used well, social media can be part of collaborative working and co-production.

This policy sets out our expectations for internet and social media use for Communitas employees and those visiting the Organisation. It outlines the ways in which staff can ensure acceptable use of the internet and social media by patients and visitors.

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 Vine (byTwitter)
- Picture sharing e.g. Flickr, Instagram and Pinterest
- Professional sharing e.g. LinkedIn
- Social bookmarking e.g. Reddit, Scoop.it, StumbleUpon and Delicious

New social media channels and platforms will emerge but the underlying principles and expectations of this policy will be the same.

2. *Purpose and Scope*

This policy applies to all personnel of Communitas Clinics, including those directly employed via an employment contract and those engaged on a self-employed basis or a contractor, volunteer, apprentice and those carrying out business at the organisation whether paid or unpaid when they are on Company premises. For the purpose of this policy, the term "personnel" will be used to describe all the above groups.

This policy also applies to patients, carers and families, and all those visiting Communitas Clinics premises whether in a personal or professional capacity. Its expectations and guidance include any use of Company or personal devices to access the internet or social media, whether through a wifi network or through alternative internet access arrangements.
The scope of this policy includes use of both Company t and personal resources to access social media, including outside of working hours. All personnel are expected to maintain a professional approach to work, patients and colleagues at all times and must not bring the Company into disrepute.

This policy is not intended to account for every situation that may arise; it aims to outline a number of important principles which reflect the standards of behaviour required by personnel of the Company.

All personnel must read and understand this policy to be clear about the general standards of conduct required when using the internet or social media. If any personnel have any doubts about the meaning of the examples listed, they should speak to their line manager for clarification.

This policy is available on the Company website and forms part of all staff induction to make personell, patients and visitors aware of this policy and it's guidance.

3. *Definitions*

Social media is 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 is 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 is 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 which limits messages (or "tweets") to 280 characters in length.

Blogging is 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 is 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 is a form of social networking website which 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.

4. Duties

Managers
All Trust managers are responsible for ensuring that personnel know how to access current Company policies and that where these are not being adhered to, discuss the standards and expectations required with staff concerned.

All managers must understand the policy and how to escalate concerns that cannot be locally resolved.

Personnel
All Communitas personnel are required to adhere to this policy.

All personnel have a responsibility to report inappropriate use as outlined in this policy to their line manager in the first instance or to another member of staff (as outlined in 9.0)

Patients and Trust visitors
All patients and Trust visitors are required to adhere to this policy. It is the responsibility of Communitas to ensure the policy is publicised and available for review by all patients and visitors.

5. Communitas use of Social Media

Communitas Clinics maintains it's own corporate presence on the following social media channels:

- Linked In
- In direct response to patient feedback on public website e.g. NHS Choices

Maintaining an active presence on social media sites allows the Communitas 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 CEO who is responsible for Communications, with support from the Business Development and Marketing Teams.

Content deemed suitable for corporate social media includes:

- News, events and activities that are related to Communitas' business
- Content that provides a direct link back to the Company's external website
- New developments, awards or achievements in the Company
- Engagement with people who have an interest in the Company
- Information that enhances the Company's reputation

Any member of staff may submit information to be considered for inclusion on Communitas' social media sites by contacting the Business Development Team. We are always looking for stories about staff, services and the people we care for. We recognise the importance of the internet in shaping public thinking about the Company and our services.

Staff are therefore permitted to interact on approved social media websites. Before using work-related social media you must:

- have read and understood this policy and the Email & Internet Policy
- have sought and gained prior approval to do so from the Senior Manager or a Director

6. *Key principles for use of social media*

These key principles apply to all Communitas Clinics' personnel or contractors who make use of any form of social media, whether personal or professional, using Trust or personal equipment, inside or outside working hours.

The intention of these principles is not to prevent personnel 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 personnel and the Company.

6.1 Maintain confidentiality at all times

All personnel have a responsibility to maintain and protect service user, colleague and organisational confidentiality. Under no circumstances should you identify service users, or post information that may lead to the identification of the individual or post information that is stigmatising or derogatory to any patient group or condition. This includes never disclosing information which may be:

- Sensitive
- Confidential, or
- Subject to a non-disclosure agreement

Staff using social media for work purposes can be only held liable for a breach under the DPA, if the breach is wilful (S55); otherwise the Company is liable as Data Controller.

If you do disclose any such information, then you interfere with privacy and breach the law on confidentiality, your employment contract and your professional Code of Practice.

When creating a new social media account a privacy impact assessment should be completed to ensure that the Company's information governance standards are adhered to. The PIA will form part of the guidance and support provided to staff using social media channels.

6.2 You are an ambassador for the Company and your profession

Never post a comment, photo or video online that you would not be willing to share with people in "real" life in a face-to-face setting.

Your online behaviour not only reflects on you, but also on the Company and your profession. While there is often a focus on the negative impact of social media on an organisation and its reputation, remember that you have the potential to act as a positive and respected ambassador for the Company.

Everything you post 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. Presume that everything you post online will be permanent and will be shared.

You should refrain from any action or activity which may bring you, your colleagues, your profession, the organisation or the NHS into disrepute. This may include posting on any social media (whether text, images, video or audio) that expresses defamatory, derogatory or offensive comments or attitudes (whether explicit or implied) towards:

- Service users, their relatives, carers or visitors

- Your colleagues, direct reports or managers
- The company, or its contractors

6.3 Be mindful of professional boundaries

Do not use social media to build or pursue relationships with service users, their families or carers even if they are no longer in your care. If you receive a friendship request from a current or former patient or their relative, some sites like Facebook allow you to ignore this request without the person being informed, avoiding unnecessary offence.

6.4 Protect your own privacy

Think carefully about what kind of information you want to share and with whom, and adjust your privacy settings accordingly. For example, on Facebook you can adjust your privacy settings at group level to share different levels of information with different groups of friends. Remember that the more your personal life is exposed through social media, the more likely it is that this could have a negative impact on you and your reputation and that of the Company.

6.5 Employee 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.

Communitas acknowledges that social media provides a number of benefits in which personnel may wish to participate. Whether or not an employee explicitly declares their association with Communitas on social media, they are expected to behave appropriately and professionally at all times, and in a manner which is consistent with the company's values and policies and relevant professional codes of conduct.

Communitas and individual professional bodies have issued specific guidance to their members in relation to the use of social media:

- Royal College of Nursing (RCN)
- Nursing and Midwifery Council (NMC)
- Health and Care Professions Council (HCPC)
- General Medical Council (GMC)
- British Medical Association (BMA)

Personnel 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

The absence of affiliation or registration with a professional body (e.g. where registration is not required for employment), does not exempt personnel from appropriate and responsible use of social media

Personnel who are found to breach the Internet and Social Media Use Policy or the Company's Acceptable Use Policy may be subject to disciplinary action in line with the Company's Disciplinary and Capability Policies.

6.6 Bullying and Harassment

The use or social networking or blogging sites to bully, harass or intimidate other employees of the Company will lead to investigation and may result in disciplinary action being taken. Staff who have concerns about this should contact their line manager or HR with a copy of the relevant content.

Staff can also take action themselves to block 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.

7. PATIENT / VISITOR USE OF INTERNET AND SOCIAL MEDIA

Patients and visitors to Communitas sites will be able to access guest wifi where avialable. The appropriateness of accessible content will be automatically managed by the IT team using existing security protocols.

Patients and visitors may be able to access social media and internet sites via their mobile phone networks whilst at clinic sites, which are not subject to the same security protocols.

Where staff suspect inappropriate use of social media or internet content by patients or visitors, they should alert their line manager in the first instance.

The company requires all users of mobile devices to use them in a courteous, considerate and non-intrusive manner to help maintain a caring environment and effective working environment for staff. Patients must not use mobile devices during consultations with communitas staff.

Mobile devices must not be used to photograph staff, patients or facilities without the explicit permission of the individual and the ward/department manager.

Patients may take photos of themselves and/or their relatives for personal reasons, and for their own personal use only. Patients and visitors must ensure that other patients are not visible in any part of such photography, to ensure confidentiality and to protect privacy and dignity.

Express permission is needed for photographs to be taken of the inside of hospital premises, particularly wards and clinical areas (including Communitas staff). This should be obtained from the service manager or service lead in the first instance. Taking photographs on our site of other patients, staff or visitors without their informed consent is not permitted.

We understand that our patients will want to stay in touch with their friends and family while in our care. We also have a duty to protect patient confidentiality and a responsibility to safeguard vulnerable patients in our care. The following guidelines apply to all our patients:

- You may overhear conversations about other patients while in our clinics. Please respect the confidential nature of these conversations by not sharing details about others in our care without their prior consent. If we obtain evidence of internet or social media activity that shares such confidential information, we will ask you to remove that content.
- Defamatory comments about members of our staff should not be shared in any public forum. Legal advice will be sought and action taken where necessary.

8. USING SOCIAL MEDIA IN DEPARTMENTS AND SERVICES

The company's official social media presence is managed by the Business Development team. This team is authorised to publish content on social networking and blogging sites on behalf of the Company.

A team may decide that there would be a beneficial and positive use for social media as a means of communication and engagement with service users and/or carers within their service area. Teams should not set up or use social networking pages or sites to represent the Company unless authorised to do so by the Business Development Team.

To ensure teams fully understand the benefits, risks and the resource needed to manage these accounts, they will be asked to complete a business case for setting up a service-specific social media account. The Business Development team can provide the business case form and will consider it when completed before service accounts are set up. Part of this process will be to complete a Privacy Impact Assessment.

8.1 Credentials

Where staff have been authorised to use social media on behalf of the Company, all account profiles on the social network or blog will belong to the Company , including login credentials and information which allow the Company to access and use the social account.

These are required to be handed over to the Company on request and arrangements must be made to transfer ownership (including account passwords and related email accounts) to the Company when the member of staff concerned is on annual or sickness leave or before that member of staff leaves the Company permanently.

8.2 Content

The Business Development team will provide advice, guidance and training to teams on setting up and managing their social media accounts, including standard responses to enquiries.

Ad-hoc checks regarding content will be taking place. If using copyrighted content, teams should mention their source or ask for authorization to use the content.

All pages, accounts, profiles or groups must display a disclaimer as per guidance.

All social media accounts managed by service teams will be expected to adhere to this policy and all other relevant Company policies. The Company will take steps to remove any account or content that operates outside this policy.

9. Raising a concern

Personnel who become aware of a breach of this policy have a duty to report it to their line manager. If they are unable to or are uncomfortable doing so, they may report their concerns to the next in line, another senior manager or via mechanisms outlined in the Company's Whistleblowing Policy.

Personnel who become aware of inappropriate use of the internet or social media by patients or visitors on Trust sites should report it to their line manager.

Line managers who are made aware of a breach of the policy should seek Human Resources (HR) advice and where possible resolve the matter informally and locally. Where it concerns patients or visitors, line managers should seek advice from the Safeguarding Teams if required and where possible resolve the matter informally and locally.

Directly employed personnel in breach of the policy will be managed via the company's Disciplinary and Capability Policies and sanctions taken could include dismissal.

If you feel that you are the target of complaints or abuse on social media sites, you can remove someone from your friends or followers list and block them from interacting with you. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others. If you have reason to believe that the activity is originating from a colleague or service user, you should alert your line manager or the next in line. Any grievance with the Company should be channelled through procedures and policies already in place and dealt with in the work environment, and not displayed or discussed via social media.

10. Dissemination and Implementation

Once agreed, this policy will be disseminated to personnel via email and made available to all staff via the Communitas Website.

The policy will be made available to visitors, patients, and carers on the company website.

11. Monitoring and review of this policy

The Senior Manager, shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice.

12. VERSION HISTORY TABLE

VERSION	DATE UPDATED	UPDATED BY	REASONS
1.1			Reviewed by DPO and AB – no changes required