


POLICY DOCUMENT

Policy Title:	Mobile Computing, Bring Your Own Device and Social Media Policy
Policy Group:	Information Governance and Administration
Policy Owner:	Information Services Manager
Issue Date:	2 nd March 2022
Review Period:	24 months
Next Review Due	2 nd March 2024
Author:	Simon Burchell
Cross References:	Information Governance Policy Staff Handbook D4-7, D10, D30 Acceptable Use for Hospital Wi-Fi Services Policy Infection Prevention and Control Policy Internal Communication Policy
Evidence:	IGA Use of Mobile Devices in Hospitals IGA BYOD Information Governance Guidance Using Mobile Phones in NHS Hospitals Jan 2009 (DH) NHS Your Guide to Using Social Media in the NHS Nov 2014 GMC Doctors' Use of Social Media
How implementation will be monitored:	Supervision by Senior Nurses and other managers
Action to be considered in event of a breach:	Disciplinary procedure for staff. Incident report to be prepared if visitors refuse to comply with this policy.
Computer File Ref.	O:/risk management/Policies/Information Governance
Policy Accepted by MT	2 nd March 2022
Sign-off by CEO	

Purpose of Policy:

The purpose of this policy is to clarify in what circumstances mobile computing devices, including phones, may be used on site by staff, patients and visitors. This policy supersedes the Mobile Phone Policy.

Policy Statement:

With the provision of Wi-Fi throughout the Hospital, mobile device use has been actively encouraged. Wi-Fi allows patients, visitors, and staff to access the internet using their own smartphones, tablets, and laptops. Wi-Fi also allows the provision of full Hospital network access to approved mobile devices. The staff intranet also encourages staff to use their own devices at work.

Use of Hospital-owned mobile devices can pose an information security risk, in that devices may be lost, damaged, or stolen, potentially resulting in loss or inappropriate disclosure of data. When using such devices, the risks of working in an unprotected environment must be considered and mitigated where possible by the use of appropriate security systems and the procedures in this policy. The use of social media can also be a significant confidentiality risk.

Monitoring social media use

Hospital IT and internet resources — including computers, smart phones and internet connections — are provided for legitimate business use. The Hospital therefore reserves the right to monitor how social networks are used and accessed through these resources. Any such examinations or monitoring will only be carried out by authorised staff. Additionally, all data relating to social networks written, sent or received through the Hospital's computer systems is part of the official records of Holy Cross Hospital. The Hospital can be legally compelled to show that information to law enforcement agencies or other parties.

Potential sanctions

Breaches of this policy may be subject to disciplinary action. Staff, contractors and others may also be held personally liable in some instances, and the Hospital will involve the police or other law enforcement agencies if necessary.

This policy should be read alongside other key policies. The Hospital's Information Governance Policy and Acceptable Use Policy for Public Wi-Fi Services are particularly relevant to staff using social media.

Equality & Diversity

This policy has been reviewed for overt or implied discrimination within the scope of the Hospital's policies on equality and diversity and none was found.

Review

The policy will be reviewed biennially to ensure that the system described continues to provide an effective framework for managing mobile computing and social media.

A1 USE OF PERSONAL MOBILE COMPUTING DEVICES

Mobile device usage on the hospital site needs to be restricted to ensure that the patients' environment remains free from noise and intrusion, and from the risk to confidentiality and privacy arising from the use of cameras in mobile devices.

Ward staff must not carry personal mobile devices whilst on duty unless they have been specifically authorised to do so. All personal mobile devices should be switched off while in the Physiotherapy Departments and Hydrotherapy.

Staff may bring their own devices for use during breaks away from clinical areas. Personal mobile devices may connect to the Hospital's public Wi-Fi but are not permitted on the Hospital's LAN Wi-Fi. The use of a personal devices for work purposes is limited to consulting the staff intranet, retrieving personal documents or photos to forward to a hospital email address for work use, or any other authorised purpose.

Any member of staff who brings their own device to work must agree to allow the Hospital to examine data stored on the device should that be requested, and must observe the following rules:

1. No patient data may be stored on a personal device, in particular photos, video, and voice recordings.
2. Personal devices may connect to our public Wi-Fi but may *not* connect to the Hospital LAN network.
3. Authorised users may be permitted to connect to their Microsoft Outlook 365 account. Personal devices connecting to Microsoft Outlook 365 accounts must be encrypted. Remote/personal access to Outlook 365 accounts is only possible when specifically enabled by the Information Services Manager.
4. The Hospital is not liable for damage to personal devices or data stored on them.
5. Visiting medical staff may need to take emergency medical calls, and so they are permitted to carry and use personal mobile phones whilst in the hospital, but must do so with due consideration to patients' privacy and dignity and the health and safety risks.
6. Patients and their visitors may use mobile phones whilst in their rooms to make telephone calls so long as such use does not unreasonably hinder staff carrying out their duties. Patients and visitors are not allowed to take photographs without the authority of a senior manager.

A2 USE OF PERSONAL SOCIAL MEDIA

Wi-fi allows access to social media in the Hospital. This policy therefore includes rules governing the use of personal social media accounts at work, what staff should not say about the Hospital on personal social media, and how authorised users will use the Hospital's social media accounts (see section E).

Definition of Social Media

Social media are web-based applications that allow the creation and exchange of content. This includes blogs and microblogs (such as Twitter), internet forums (such as nursingforum.co.uk), content communities (such as YouTube and Flickr), and social networking sites (such as Facebook and LinkedIn).

Summary

Social media use can bring significant benefits. However, it is important that staff who use social media do so in a way that does not damage the Hospital's reputation. A misjudged status update can generate complaints, or violate data protection laws. This policy therefore includes guidance on how to use social media safely and effectively (see Appendix 2).

Scope

The policy applies to all staff, contractors and volunteers who use social media while on site, whether for business or personal reasons, or elsewhere if the Hospital is mentioned.

Responsibilities

- The Chief Executive is responsible for ensuring that the Hospital uses social media safely and in line with its objectives and values.
- The Information Services Manager is responsible for providing apps and tools to manage the Hospital's social media presence, for tracking key performance indicators, and for monitoring for social media security threats.
- The Chief Executive is responsible for working with contractors to roll out marketing ideas and campaigns through social media channels.
- The Information Services Manager is responsible for ensuring requests for assistance and support made via social media are followed up.

Personal Social Media Accounts

Staff may not access personal social media accounts on Hospital-owned equipment, except in the normal course of their duties.

Staff may access their personal social media accounts on their own devices via the Hospital public Wi-Fi service when they are on a break or off duty, but must always maintain Hospital confidentiality standards. Staff may not mention patients, or post photographs of patients or clinical areas. Nothing should be posted on social media accounts that could not normally be said in a public setting, or that would contravene confidentiality rules or professional codes of conduct.

B. PATIENTS AND VISITORS

Always consider if the current episode of social media use is in the patient's best interest. A family member or a relative appointed as a Power of Attorney or Court of Protection Deputy should be consulted before a relative or a friend involves a patient in social media conversation/ call.

Low intrusion areas

Areas have been identified within the Hospital where considerate mobile device use is acceptable. These areas are:

- Hospital Reception and Entrances
- Staff dining room
- Offices
- A patient's private room

Use of mobile devices for photography or video recording in these or any other areas is not permitted without the authority of a senior manager.

Use of Mobile Devices by Patients and Visitors

Patients, their relatives, and other visitors, will at times use mobile devices including smartphones, tablets, and laptops. These devices may be used where such use does not impinge upon patient privacy, confidentiality, and safety. Recording of any kind on any device may not take place without the approval of a senior manager. These devices may connect to the public Wi-Fi service provided by the Hospital but are not permitted on the Hospital's LAN Wi-Fi.

See also Appendices 4 and 5.

C. USE OF HOSPITAL-OWNED MOBILE COMPUTING DEVICES

Hospital owned laptops and devices are in regular use within the Hospital, including for training and presentations. Some teams regularly use tablets in the course of their duties, and laptops are often used during meetings, for video calls, and for working from home.

As of April 2020 the Hospital owns 16 Windows laptops, 9 Android tablets, 2 iPads, 4 Windows tablets, 1 Amazon tablet and 7 smartphones. A donated iPad is not authorised for clinical use; a purchased iPad is integrated with the server security software and authorised for clinical use. All devices and their serial numbers are recorded on the IT Assets database.

Off-site use of Hospital-owned mobile computing devices

Hospital-owned mobile computing devices may not be taken offsite without authorisation of the Chief Executive or the Information Services Manager. Any device taken offsite must have encryption in place. Loss or theft of the device must be reported immediately to the Information Services Manager.

Managing infection risk

Precautions are required to ensure the safety of patients when using equipment such as mobile phones and computer keyboards or tablets. The precautions include hand washing before direct contact with patients and after any activity that contaminates the hands, and regular cleaning of the equipment with disinfectant wipes, which should be used in line with manufacturer's instructions.

Charging of Hospital-owned mobile computing devices

Due care must be taken when charging devices in the Hospital.

1. No medical equipment must be unplugged in order to charge a device.
2. No leads should be left trailing in such a way that they present a trip or tangling hazard.
3. All devices must undergo PAT testing before being connected for the first time.

Training

All users of hospital-owned mobile devices must have attended IT Induction training and Information Governance training.

D. USE OF PERSONAL SOCIAL MEDIA ACCOUNTS FOR WORK PURPOSES

Holy Cross Hospital recognises that use of personal social media accounts can have benefits. For instance, staff can make contacts that may be useful in their jobs and can find content to help them learn and develop in their role.

Accordingly, staff are allowed to use their personal social media accounts at work, subject to approval of their line manager and to the rules set out below.

Personal social media rules

Acceptable use:

- Staff may use their personal social media accounts for work-related purposes during regular hours, but must ensure this is for a specific work related purpose (for example, for clinical research).
- Use of social media accounts for non-work purposes is restricted to breaks.

Talking about the Hospital

- Staff should ensure it is clear that their personal social media account does not represent the Hospital's views or opinions.
- Staff may wish to include a disclaimer in their social media profiles: 'The views expressed are my own and do not reflect the views of my employer.'

Safe, responsible social media use for work purposes

The rules in this section apply to:

- Staff using Hospital social media accounts
- Staff using personal social media accounts during working hours for work purposes

Staff must not:

- Create or transmit material that might be defamatory or incur liability for the Hospital.

- Post message, status updates or links to material or content that is inappropriate. Inappropriate content includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- Use social media for any illegal or criminal activities.
- Send offensive or harassing material to others via social media.
- Broadcast unsolicited views on social, political, religious or other non-business related matters.
- Send or post messages or material that could damage the Hospital's reputation.
- Interact with competitors in any ways which could be interpreted as being offensive, disrespectful or rude, and communication with competitors should be kept to a minimum.
- Discuss colleagues, competitors, patients or suppliers without their approval.
- Post, upload, forward or link to spam, junk email or chain emails and messages.

Copyright

Holy Cross Hospital respects and operates within copyright laws and so users should not use social media to:

- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party. If staff wish to share content published on another website, they are free to do so if that website has obvious sharing buttons or functions on it.
- Share links to illegal copies of music, films, games or other software.

Security and data protection

Staff should be aware of the security and data protection issues that can arise from using social networks.

Maintain confidentiality

Staff must not:

- Share or link to any content or information owned by the Hospital that could be considered confidential or commercially sensitive, such as future plans.
- Share or link to any content or information owned by another company or person that could be considered confidential or commercially sensitive.
- Share or link to data in any way that could breach the Information Governance Policy.

Avoid social scams

- Staff should watch out for attempts to use deception to obtain information relating to the Hospital, and avoid revealing any personal or sensitive details through social media channels.
- Staff should avoid clicking links in posts, updates or messages that look suspicious.

E. USE OF HOSPITAL SOCIAL MEDIA ACCOUNTS

This part of the social media policy covers use of social media accounts owned and run by the Hospital.

Authorised users

Only staff who have been authorised to use the Hospital's social networking accounts may do so. Authorisation is usually provided by the Information Services Manager, and is typically granted when social media-related tasks form a part of the job description. Allowing only designated people to use the accounts ensures the Hospital's social media presence is consistent and cohesive.

Creating social media accounts

New social media accounts in the Hospital's name must not be created unless approved by the Information Services Manager.

Inappropriate content and uses

Hospital social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the Hospital into disrepute. When sharing an interesting blog post, article or piece of content, staff should always review the content thoroughly, and should not post a link based solely on a headline. Further guidelines on use can be found below.

Purpose of Hospital social media accounts

The Hospital's social media accounts may be used for a variety of purposes. In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the Hospital's overall objectives.

For instance, staff may use the social media accounts to:

- Respond to enquiries and requests for help
- Share blog posts, articles and other content created by the Hospital
- Share insightful articles, videos, media and other content relevant to the Hospital's business
- Provide supporters or followers with an insight into what goes on at the Hospital
- Promote marketing campaigns and special offers
- Support new service launches and other initiatives

Protection of Hospital social media accounts

- Hospital social media accounts should be protected by strong passwords that are changed regularly and shared only with authorised users.
- Staff must not use a new piece of software, app or service without receiving approval from the Information Services Manager.

F. Virtual Assistant Technology

Virtual assistants are interactive Artificial Intelligence programs either running from a PC, laptop, tablet or smartphone, or via a dedicated device. The microphone for virtual assistants is always switched on so it can pick up voice commands, and data can be stored indefinitely on external servers. Virtual assistants include Amazon Alexa, Amazon Dot, Amazon Echo, Apple Siri, Google Assistant, Microsoft Cortana and many more.

The use of such technology in hospital presents significant data protection concerns. Data is stored on external servers, and the appropriate measures have not been put in place to protect patient information. The use of such technology has the potential to significantly improve the quality of life of severely disabled patients. Such devices may be used with the following safeguards:

- Clear signage on the door of any patient room containing a virtual assistant
- The patient's care plan being updated to include the usage of the virtual assistant
- At any time that a clinical conversation or any other confidential conversation is taking place in a room with a virtual assistant, the device must be switched off at the wall

G. Remote email access

Approved users are granted remote access to their Microsoft Outlook email account. This access is permitted from both hospital-issued smartphones and personal smartphones, and is configured with the assistance of the Information Services Manager. Any device used to connect to hospital email must be encrypted.

H. Remote working

The Hospital has enabled remote working for approved users. Approved users are issued with a hospital-owned laptop which is tethered electronically to a desktop PC in the Hospital. The laptop becomes a remote portal for accessing the office PC. Both the laptop and the PC need to be configured by the Information Services Manager in order for remote access to function.

Remote working is only permitted on Hospital-owned equipment with the appropriate security measures in place, such as encryption, virus protection and data loss prevention software. Users who are granted remote working privileges must take all reasonable steps to ensure that their device is secure, for their own use only, and be vigilant as to who may see their screen when viewing confidential information.

Appendix 1

Risks and Restrictions on Mobile Devices

Mobile device use is subject to approval by senior clinical staff in all clinical areas. Staff may be authorised to use Hospital-owned devices in the course of their duties. Senior staff may prohibit the use of mobile devices by visitors in any part of the hospital or its grounds if they assess that such use is a threat to the welfare, dignity or privacy of patients.

Mobile device use is forbidden or restricted in clinical areas for the following reasons:

1. Patient privacy and dignity: To eliminate any possibilities that mobile devices are used for communicating confidential information, or video or audio recording patients, or photographing patients or other people in the Hospital.
2. Cross Infection: Mobile devices are known to harbour bacteria that can be transmitted to patients or to food.
3. Inappropriate display of confidential information in a publicly viewable area.
4. Unattended LAN-enabled device allows unauthorised network access.
5. Disturbance in the environment: Wards and treatment areas are places of treatment, rest and recuperation. Patients have a right to enjoy a peaceful environment and to receive services from staff who are not unnecessarily distracted. Mobile phone ring tones, conversations, unwanted music, and streamed video are all intrusive and may have an adverse effect on the environment for other people.
6. Health and safety risks include electrical risks from using untested and possibly defective chargers, inadvertently unplugging essential equipment and being distracted by a device when carrying out work that requires full attention, such as driving or operating machinery or equipment.
7. Damage to device by dropping or rough handling.
8. Confusion with alarms with resultant health and safety risks. The variety of mobile device ring tones could cause confusion for clinical staff between a ring tone and a genuine medical equipment alarm signal that requires urgent attention.
9. Trailing leads (including power leads, visual display leads, microphones, headphones etc.) present a trip or tangling hazard.

Appendix 2

Basic advice on using social media

Regardless of which social networks employees are using, or whether they're using business or personal accounts on company time, following these simple rules helps avoid the most common pitfalls:

- Know how the social network works. Staff are advised to spend time becoming familiar with the social network before contributing. It's important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.
- If unsure, don't post it. Staff should err on the side of caution when posting to social networks. If it is felt that an update or message might cause complaints or offence — or be otherwise unsuitable — then don't post it. Staff members can always consult the Information Services Manager for advice.
- Be thoughtful and polite. Many social media users have got into trouble simply by failing to observe basic good manners online. Staff should adopt the same level of courtesy used when communicating via email.
- Look out for security threats. Staff members should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. Further details below.
- Don't make promises without checking. Some social networks are very public, so staff should not make any commitments or promises on behalf of Holy Cross Hospital. Any Hospital related enquiries should be directed to the Information Services Manager.
- It is best to handle complex queries via other channels. Social networks are not a good place to resolve complicated enquiries and issues. Once an external person has made contact, staff should handle further communications via the most appropriate channel, which is more usually email or telephone.
- Don't escalate matters. It's easy to post a quick response to a contentious status update and then regret it later. Better to think before responding, and hold back if in any doubt at all.

Appendix 3

Advice for Patients and their visitors on the use of Virtual Personal Assistant technology

Virtual assistants are interactive Artificial Intelligence programs either running from a PC, laptop, tablet or smartphone, or via a dedicated device. The microphone for virtual assistants is always switched on so it can pick up voice commands, and data can be stored indefinitely on external servers, which can be anywhere in the world. Virtual assistants include the following, and many more:

- Amazon Alexa
- Amazon Dot
- Amazon Echo
- Apple Siri
- Google Assistant
- Microsoft Cortana

Since the microphone is always switched on, it may potentially overhear confidential conversations between healthcare staff, patients and visitors. It is not possible to know where that information is stored, how it could be accessed, or by whom. This technology therefore represents a threat to confidentiality in the hospital.

With this in mind, we require that all Virtual Assistants are registered with Information Services. There should be clear signage on the door indicating that a Virtual Assistant is in use. The Occupational Therapist will ensure that the patient's care plan is updated with guidance regarding the Virtual Assistant. Whenever a clinical or otherwise confidential conversation is taking place in the patient's room, the device must be switched off completely.

Appendix 4

Using Social media: Information sheet for patients and relatives

Introduction:

Interactive social media technology has revolutionised the way people connect and interact. Facebook, Twitter, Flickr, blogs, instant messaging and photo and video exchange sites are increasingly popular and provide an opportunity to connect with people. However, the use of social networking sites also introduces a range of potential safeguarding risks to vulnerable adults.

As organisations increasingly use social networking and other developing media to communicate with people it is critical that safeguarding protocols and practices keep pace with the raft of communication methods young people use. It is recognised that when working with vulnerable adults, their capacity to make specific decisions must be taken into consideration when applying these guidelines. This will ensure that vulnerable adults are able to exercise choice and freedom whilst being encouraged to make decisions which promote their safety.

When using social media services:

1. Recognise that this medium provides opportunities to effectively engage with a wide range of audiences
2. Understand the potential safeguarding risks of using social media
3. Familiarise yourself to safety tools provided by social networking service providers and their acceptable use policies.

The aim of this document is to provide basic information about social media, highlight potential risks to patients and signpost you to some useful websites that advice on safe use of social media.

Social media refers to the latest generation of interactive online services such as blogs, discussion forums, pod casts and instant messaging. Social media includes:

- Social networking sites e.g. Bebo, Facebook, Piczo, Hi5 and MySpace
- Micro-blogging services e.g. Twitter
- Video-sharing services e.g. YouTube
- Photo-sharing services e.g. Flickr
- Online games and virtual reality e.g. Second Life

Skype is an instant messaging app that provides online text message and video chat services. Users may transmit both text and video messages and may exchange digital documents such as images, text, and video. Skype allows video conference calls. Features of various social networking sites is listed in Appendix 2

Benefits to patients from using Social media:

Patients with capacity

- Keeping in touch with family and friends
- Identify services (Leisure etc) that they are interested in
- Help patients engage, connect and develop unique interaction with people in a creative and dynamic medium where users are active participants
- Patients can get details of events or campaigns of interest
- Provide patient with information related to their condition and treatments

Patients without capacity

- May help with visual and auditory stimulation and increase awareness with familiar sounds/ voices
- Change of environment/ setting

Always consider if the current episode of social media use is in the patient's best interest. A family member or a relative appointed as a Power of Attorney or Court of Protection Deputy should be consulted before a relative or a friend involves a patient in social media conversation/ call.

If you need advice regarding a patient's participation in social media or would like to clarify before uploading content in a social media platform, please feel free to speak to a senior clinical manager

Benefits to relatives

- For relatives living far afield, Social media provides an easy to use, low cost medium to keep in touch with their loved ones.
- Social media could help find support organisations where you may find other members who are relatives of people with similar conditions

Potential risks to patients

Patients with capacity

- bullying by peers and people they consider 'friends'
- posting personal information that can identify and locate a child, young people and vulnerable adults offline
- sexual grooming, luring, exploitation and abuse contact with strangers
- exposure to inappropriate content
- involvement in making or distributing illegal or inappropriate content
- theft of personal information
- exposure to information and interaction with others who encourage self-harm
- exposure to racist or hate material
- encouragement of violent behaviour, such as 'happy slapping'
- glorifying activities such as drug taking or excessive drinking

Patients without capacity

- Risk of abuse and exploitation due to
 - inability to consent to participate or being broadcasted through video call
 - inability to remove themselves from the situation
 - inability to block/ untag/ report abusive contacts