Personal Use of Social Media Guidance

Co-ordinator:	Reviewer:	Approver:
Senior Communications Officer, Corporate Communications Information Security Officer, eHealth	GAPF Policies Subgroup	Grampian Area Partnership Forum (GAPF)

Date Approved by GAPF:	Review date:
10 August 2017	31 December 2022

Uncontrolled when printed

Version 2

The provisions of this policy, which was developed by a partnership group on behalf of Grampian Area Partnership Forum, apply equally to all employees of NHS Grampian except where specific exclusions have been identified.

NHS Grampian
Personal Use of Social Media Guidance

This document is also available in large print and other formats and languages, upon request. Please call NHS Grampian Corporate Communications on Aberdeen (01224) 551116 or (01224) 552245.

This Policy has undergone Equality and Diversity Impact Assessment.

Revision History:

Document Title	Policy Version	Date Approved by GAPF	Review Date
Personal Use of Social Media Guidance	2	10 August 2017	Amended to 31 December 2022

NHS Grampian
Personal use of Social Media

Contents

1.0 Introduction

Social media is online technology that enables the sharing of information, the promotion of discussion and the establishment and development of relationships. It can be accessed through websites on computers or via special applications on mobile devices.

Information can be shared in a variety of different formats, such as text, pictures, video and audio. Examples of popular social media sites include Facebook, Twitter, Whatsapp, Snapchat, Tumblr, Wordpress, YouTube, Google+, Vine, Blogspot and LinkedIn. This list is not exhaustive and this guidance is not limited to these platforms alone.

NHS Grampian acknowledges that many employees visit and participate on social media sites in a personal capacity, mostly without problems or incident. Social media is an excellent tool to share learning, celebrate success and communicate directly with people across Grampian. If you wish to use social media in a professional capacity there is a separate policy (Social Media for Business Use); please refer to that.

Every employee is free to choose which social media they participate in and to what extent. However they must bear in mind that they represent NHS Grampian in their daily lives. Their personal and professional lives should remain separate and anything posted on social media should not be seen to bring NHS Grampian into disrepute. As such NHS Grampian recognises the need to provide clear guidelines for all of its employees on the appropriate personal use of Social Media in order to safeguard the reputations of the employee, other individuals and the organisation.

The intention of this guidance is not to interfere with an employee's personal life or to discourage them from using Social Media outside of work. The aim is to highlight the potential risks and issues that can arise due to inappropriate use of these sites and the consequences this could have on an individual's employment with NHS Grampian. NHS Grampian will not monitor an employee's social networking sites and does not intend to be prescriptive about how employees should conduct themselves in their private lives. However, where material is brought to the attention of the organisation which may be considered to be inappropriate NHS Grampian will investigate in line with the appropriate policy or legislation.

2.0 Scope

This guidance applies to all employees of NHS Grampian and others carrying out work for NHS Grampian such as contractors, volunteers, honorary and other contract holders.

Members of staff who use personal communications devices should refer to and comply with the NHS Grampian Electronic Communications Protocol.

This guidance concerns the personal use of social media sites during hours of work, rest breaks and when employees are not at work.

3.0 Guidelines for staff on the appropriate personal use of Social Media
Remember: You are personally responsible for any content you publish/post - the views and opinions you express are your own and not those of NHS Grampian.

Staff are strongly advised:

1. **To think before you publish/post.**

   Whether you are posting a status or message of your own or sharing content from other people, take a moment to think about how others might react. Posted content can be difficult to retract and can spread very quickly through social media sites if it is circulated by other users. It can become permanently available for others to see and use elsewhere. Comments, tweets, blog posts or status updates can also be used by local and national media without your permission.

   If in doubt, don't post it.

2. **To refrain from using 'NHS Grampian' or your NHS.NET e-mail address in your account title, settings or profile in any form.**

   If you do identify yourself as an employee of NHS Grampian, please be aware that all comments you make reflect on this organisation. Adding a disclaimer such as 'all views my own' will not preclude disciplinary action being taken against you for inappropriate posts. Work e-mail addresses should not be used to register for personal social media accounts.

3. **To comply with existing policies**

   Adhere to the appropriate conduct policies as well as (if applicable) the codes of conduct relevant to your profession (for example The Nursing and Midwifery Council, The General Medical Council and The Health and Care Professions Council). Staff are reminded of their own obligations to comply with all relevant UK legislation and the terms and conditions of acceptable use that each social media site has in place.

4. **Not to attempt to access social media sites on NHS Grampian PCs or devices – unless you have the appropriate authorisation to do so for work purposes**

   The majority of social media sites are blocked on the NHS Grampian network. Attempts at unauthorised access may contravene the Information Security Policy, resulting in possible action under the relevant employee conduct policies. If you wish to use social media for work purposes it is possible to apply for access. Details of how to do this can be found in the NHS Grampian Social Media for Business Use Policy.

5. Not to post messages, images or recordings of patients or colleagues.

In addition, do not publish content about the NHS, its services, facilities, staff, patients or third parties that could be considered as inappropriate, confidential, offensive, defamatory, discriminatory, harassing, illegal, embarrassing, threatening, intimidating, which may incite hatred or compromise the safety of staff or patients.

6. Not to use social media for whistle blowing or to discuss any aspect of your work.

Social Media is not the appropriate place to raise or discuss work matters or issues. Any legitimate concerns should be addressed through the appropriate policies.

7. To choose your online friends wisely.

Do not accept 'friend' or 'follow' requests from patients you have only come into contact with during the course of your work, or their friends or relatives.

Before 'liking' or 'following' others (and deciding whether to permit others to 'like' or 'follow' you) consider whether you wish to be associated with that person/brand/organisation and their views and values – carefully consider any potential consequences or repercussions that could arise from such association. Avoid any conflict of interest.

8. To keep your account secure and check your privacy settings.

Make sure you are fully aware of the account settings on your Social Media account and that you regularly review these settings to maintain your security and privacy.

Social media sites are regularly targeted by hackers trying to get access to users' accounts. To help keep your account secure, use a complex password for signing in to your account and consider changing this regularly (such as every three or four months). Consider using login verification with each site where a security code is sent to your phone each time there is a login attempt.

Please remember that even the strictest privacy settings have their limitations. Regardless of the settings you have in place, once something is published online it can be copied and redistributed by other users very quickly and effortlessly – even if the posts you publish aren't public or are posted via a site's private messaging facility.

It is recommended that your check your settings after each application update as these can change frequently.

Be aware that many online games, puzzles or surveys require you to give them access to your account. Regular checks of your privacy and security settings will keep your account and information safe.

9. To regularly monitor content on your account.

Pay particular attention if others have access to publish/share content which will appear on your account. Other users can tag your account profile in their posts and include you in group conversations. Remove any content that others publish and take steps to disassociate your account from other posts and group conversations that could be considered to be inappropriate.

10. To report anything that gives you cause for concern

Social media sites each have their own terms of use guidelines and an option for reporting or flagging content. If you see something that may be breach of these guidelines – in particular Section 3.0, paragraph 5 – you should report it to the social media site where the content has been posted. NHS Grampian is unable to raise concerns on behalf of individual employees; you are responsible for flagging inappropriate comment. Check the rules for a particular social media site before submitting a report and be aware that content will only be taken down if a social media site agrees that another user has breached their rules. Please refer to the following links for guidance:

Facebook
Read Facebook rules - https://www.facebook.com/communitystandards
Report to Facebook - https://www.facebook.com/help/181495968648557/
Facebook safety centre - https://www.facebook.com/safety

Twitter
Read Twitter rules - https://support.twitter.com/articles/18311
Report to Twitter - https://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/15789-how-to-report-violations

YouTube
Read YouTube rules - https://www.youtube.com/yt/policyandsafety/en-GB/communityguidelines.html
Report to YouTube - https://www.youtube.com/yt/policyandsafety/en-GB/reporting.html
YouTube safety centre - http://www.youtube.com/yt/policyandsafety/en-GB/safety.html

In the event of another user promoting illegal activity or behaving in a threatening manner, report it to the Police by dialling 101 – in addition to reporting it to the social media site.

Police Scotland
Keep secure online information and advice -
http://www.scotland.police.uk/keep-safe/keep-secure-online/social-media-internet-dating

4.0 Compliance

It is the responsibility of staff and line managers to ensure that they have read and understood this guidance, along with other applicable policies and professional guidelines.

Please be aware that any social media activity which results in harm, distress or loss of reputation to patients, staff or the organisation may be considered gross misconduct and potentially unlawful.

Any member of staff who is found to be in breach of the following may be subject to disciplinary action:

- NHS Grampian Information Security Policies
- Relevant employee conduct policies
- Codes of professional standards relevant to an employee's profession.

Staff who have queries about the contents of this guidance or wish to report a breach or suspected breach should contact their supervisor/line manager in the first instance, or alternatively contact the HR Operational Team through the HR hub (extension 52888 or grampian.hr@nhs.net, or contact or staff side representative. Breaches of data security will be managed by Information Security in line with the relevant protocol(s).

5.0 Review and Monitoring

This guidance will be reviewed in light of changes in technology/law/organisational structures or as required by the policy review framework.