

Policy on the Personal Use of Social Media by Staff

Author	Maggie Jamieson Head of Communications, Claims and Patient Information
Lead Executive	Chief Executive Gordon Jamieson

Development of Policy	Reviewed	Policy Review date	Reviewers/ review team
August 2014	September 2019 September 2021 February 2024	February 2026	Head of Communications, Claims and Patient Information

Document Control

Version	Date	Latest changes made by	Status	Reason for change and reviewers
3	1/2/24	M Jamieson	Draft	Review of original policy.
3	9/2/24	M Maclellan	Draft	Update review date Remove reference to smartphones and blackberrys Added 'premises/grounds' to 4.6 Addition of mental health risks of social media in Section 1 Added email etiquette and GRGR Fact or Fiction
3	12/2/24	D MacDonald	Draft	Change Data Protection Act to 2018

Document Approval – Name(s) of the Individual(s) representing the Approving Committee(s)/Group(s)

Reviewer's Name	Reviewer's Role	Date
Communications Department	Comments/Consultation	2/2/24
Director of Human Resources	Comments/Consultation	February 2024
Area Partnership Forum	Comments/Consultation/Approval	February 2024
Corporate Management Team	Consultation/Approval	March 2024

Contents

1. Introduction	Page 4
2. Purpose of this Policy	Page 4
3. Definition of Social Media	Page 6
4. Scope	Page 7
5. Roles and Responsibilities	Page 7
6. Governance	Page 12
7. Policy Review & Monitoring	Page 13
8. Appendix 1: Email Etiquette	Page 14 – 15
9. Contact details	Page 16

1. Introduction

- 1.1 This policy sets out NHS Western Isles' position on the Personal Use of Social Media by Staff. This policy applies to what is written/posted/streamed/shared on personal social media sites during work hours and also during periods when the employee is not at work or on a rest break. (Please note that the NHS Western Isles Media and Social Media Policy covers the use of social media for business purposes.)
- 1.2 NHS Western Isles recognises the universal presence and benefits of social media and welcomes its use to support communication and connection. However, the risks associated with these channels is also acknowledged. This not only includes the risk of posting or sharing something that breaches organisational policy, but the risk to individuals of excessive social media use, which can lead to mental health challenges including anxiety, depression, eating disorders and addictions.
- 1.3 An ever increasing number of employees participate in social networking sites outside of work hours. Social media tools such as blogs, wikis, social networking sites, podcasts and message boards are changing the way we are communicating, and engaging. In the majority of cases this is uncomplicated and trouble-free. The intention of this policy is not to interfere with an employee's personal life. However there are potential risks/nuisances associated with the use of social media; risks which individuals may not even be aware of.

2. Purpose of this policy

- 2.1 The purpose of this policy is to ensure that all NHS Western Isles employees, bank workers, volunteers, students and staff from commissioned services have adequate information and clear guidance to enable them to use social networking sites in their private lives appropriately in a way that ensures that their personal and professional reputation, and that of NHS Western Isles is never compromised. This policy aims to prevent any potential harm to employees, patients and the organisation from inappropriate use of social media sites.
- 2.2 NHS Western Isles employees are accountable for their actions and activities when using social networking sites and are expected to observe at

all times the standards, conduct and behaviour outlined in the following policies, guidance and legislation:

- Data Protection Act 2018
- Equality Act 2010
- NHS Code of Practice on Protection Patient Confidentiality
- NHS Scotland Bullying and Harassment Policy
- NHS Scotland Conduct Policy
- NHS Western Isles Information Governance Policies
- NHS Western Isles Media and Social Media Policy
- NHS Western Isles Communications Strategy
- NHS Western Isles Unauthorised Filming Procedure
- Freedom of Information (Scotland) Act 2002
- The Computer Misuse Act 1990
- Human Rights Act (1998)
- Abusive Behaviour and Sexual Harm (Scotland) Act 2016

- 2.3 In addition staff must adhere to the regulatory or professional codes of conduct that applies to their professional body. Application of this policy should be considered in conjunction with all other relevant organisational policies. Where staff have legitimate concerns about what is happening at work and they feel that there is an issue that NHS Western Isles should know about or look into, they should use the appropriate policy e.g. Grievance, Bullying and Harassment or Whistleblowing.
- 2.4 There is a need to provide individuals with clear guidelines (in addition to any existing professional regulatory rules, regulations, guidelines and duties that relate to communication, conduct and the use of social media) on what is considered by NHS Western Isles to be unacceptable personal use of social media by an employee, to ensure, as far as possible, that the reputations of individuals, colleagues and the organisation are safeguarded.
- 2.5 The main principle behind this policy is that conduct on-line, and conduct face-to-face, should be judged against the same high standards of integrity and behaviour which NHS Western Isles expects of its employees. Employees should think carefully about what they post on any social media sites and **be aware that social networking websites are not secure and individual privacy settings are not sufficient to stop others seeing your content/distributing your content/printing or copying and sharing your content.** Social media platforms also frequently alter their terms of usage.

3. Definition of Social Media

- 3.1 The term 'social media' is an umbrella term used to describe online technologies and practices that are used to share information, videos, photos, knowledge and opinions. Social media services and tools can involve a combination of technology, telecommunications and some form of online social interaction and can use a variety of different formats, e.g. text, images, video and audio.
- 3.2 Social media, as a term and for the purposes of this policy, includes social networking (e.g. Facebook, Pinterest, Google +, Instagram and LinkedIn), blogging/microblogging applications (e.g. 'X' (previously Twitter), Tumblr, Svbtle, Medium, Blogger, podcasts and WordPress), multimedia sharing and networking applications (e.g. YouTube, Flickr and Skype), information sharing sites (e.g. Wikipedia), forums and chat rooms/online forums (e.g. Mumsnet, dating apps, Digital Spy and iVillage), e-petitions (e.g. Change.org), videos (livecasting) and real time web communications (chat, chatrooms, video chat, instant messaging), and personal web pages. (This list is in no way exhaustive.)
- 3.3 Social networking sites enable people to maintain contact with others. However, as a result of the open nature of such sites, it is also possible for third parties to collate vast amounts of information about individuals, their families, colleagues, and personal and professional life. Though social networks may be considered to be a personal matter, this is not the same as it being private. In many cases, written conversations and images inside these networks can be found through search engines such as Google. Even in cases where only an individual's contacts can see what they write, there is a possibility that one of them will forward what is said and make it visible to a wider audience. As a result, personal conversations within social media networks should be considered public rather than private. In addition, when someone is tagged, it creates a link to their profile. Individuals can be tagged to posts created by others without prior approval of consent.
- 3.4 Staff should also be mindful about the advancement of fraud and should be cautious about games/apps that collate personal data, background, fingerprints or images to potentially use in an illegal or fraudulent manner.
- 3.5 This policy is equally applicable to the use of social media via mobile access and includes the use of applications (Apps).

4. Scope

- 4.1 This policy applies to all employees of NHS Western Isles, whether full time or part-time, whether on permanent contracts, secondments, fixed-term or bank/locum/consultancy contracts. The policy also applies to NHS Western Isles volunteers and anyone on work experience or similar.
- 4.2 This policy relates to the personal use of social media, whether during work hours (not generally permitted, unless authorised for specific business purposes) or outside of work¹. The policy should be used, as appropriate and necessary, in conjunction with other relevant Board policies including (but not exclusive to) the Dignity at Work Policy, the Communications Strategy, the Acceptable Use of IT Policy, the Equality and Human Rights Policy, Information Governance Policies and the Employee Conduct Policy. It should also, where appropriate, be considered in line with the Board's Standards of Behaviour, Corporate Values and Objectives and any relevant professional codes of conduct.

5. Roles and Responsibilities

- 5.1 NHS Western Isles will take all reasonable steps to ensure the effective governance of this policy i.e. making sure that employees are aware of this policy and their obligations relating to personal use of social media. This will be done through the Intranet, via a Finger on the Pulse staff bulletin and inclusion in the Team Brief when the policy is launched, and managers will also be required to raise awareness of the policy through their Departmental Communications Plans. If unclear, employees should seek advice from their supervisor/line manager.

Responsibilities both in and outside of work

- 5.2 **All employees are singularly responsible for any information they make available online, whether this was posted during work hours, during breaks or when not at work.** The Board considers employees to be responsible and accountable for all information they publish themselves as well as any information contained on their social media pages, groups or blogs, even if that information originated from another source (it would be expected that inappropriate information, as defined in this policy, would be removed by the employee within a reasonable time period – i.e. once it

¹ Employers are not obliged to disregard conduct simply because it occurs outside the workplace, and this also applies to the use of social media outside of work.

has been identified). Employees therefore must ensure that, when engaging in social media activity, they abide by the following standards:

5.3 Employees must not:

- Post, send, or promote (like, repost, share, etc) any information that could potentially breach patient or organisational confidentiality; constitute harassment of an individual or group or is considered discriminatory, threatening, intimidating or illegal; or constitute defamation of character or a breach of an individual's privacy.
- Post, send, or promote (like, repost, share, etc) any information that is likely to breach NHS Western Isles or NHS Scotland policies or standards; discredit services provided by NHS Western Isles; or discredit NHS Western Isles as an employer. Any such postings will be judged in terms of the likelihood of the employee's comments causing reputational damage and the scale of any such potential damage.
- Share NHS Western Isles information that is not publicly available.
- Post, send, or promote (like, re-post, share, etc) comments or images online which, as a healthcare professional and public servant, are likely to damage the reputation of the organisation/bring the organisation into disrepute, or damage the relationship and/or trust between the staff member and the organisation, bearing in mind the stated responsibility that all staff have for 'shaping, upholding and managing' the reputation of NHS Western Isles (as defined in the Board's Communications Strategy).
- Participate (like, repost, share, etc) or offer opinions online with regard to current or rumoured legal /commercial involvement of the Board.
- Post obscene material.(under the Obscene Publications Act 1959)
- Send, receive, share or post on their personal accounts images/photos/videos of NHS Scotland patients or services users in the employee's workplace/premises/grounds (unless shared from authorised NHS sites).
- Send, receive, share or post on their personal accounts images/photos/videos taken on NHS Western Isles premises without approval (unless shared from authorised NHS sites).

- Post updates and statuses on NHS Western Isles business, services, achievements and developments, on their personal social media accounts, unless it is shared from an NHS approved account, or approved in advance by the Communications Department.
- Discuss, comment on, promote (like, re-post, share, etc) any matter that relates to a complaint or claim.
- Discuss, comment on, promote (like, re-post, share, etc) work-related issues in a manner which could cause distress to individuals, damage their own reputation or that of their employer or colleagues. Any legitimate concerns should be addressed through the appropriate Board policies e.g. NHS Western Isles Grievance Policy, Dignity at Work Policy and/or local whistle-blowing procedures.
- Use social media to attack or abuse colleagues.
- Use the internet or social media to refer to or comment about colleagues, patients or the service in an abusive or harassing manner.
- Directly reply to messages from patients/service users on care/treatment/NHS matters via personal social network accounts.
- Use or copy any trademarks or logos belonging to the NHS and must not copy or display information or material which is subject to copyright legislation, without the express permission of the owner.
- Use their NHS e-mail address to register on a social network (unless approved for work-related purposes) or include their NHS e-mail address on a personal social media account.
- Use their NHS link (including e-mail address or social media site) to obtain private work, or to direct people to their own or another person's personal/private site.
- **Engage in the personal use of social media while on duty.** Employees must limit their use of social media on their own equipment to their official rest breaks, such as their lunch break/times.

- 5.4 If an employee identifies the inappropriate use of a social networking site by another employee, they have a responsibility to report this to their own line manager. Employees are advised to take screenshots of any content for this purpose. This may be used as evidence.
- 5.5 NHS Western Isles employees must be considerate of their personal and professional boundaries when accepting friend requests. If staff are in any doubt as to how this would impact on a specific situation they should seek advice from their line manager.

Additional Responsibilities when at work

- 5.6 All NHS Western Isles IT systems and services are provided as business tools. Employees who have authorised access to the internet at work are allowed reasonable personal use, provided it does not take place during the user's recorded working hours and only where it does not impact on other business users.
- 5.7 As a general rule, NHS Western Isles employees are not permitted access to social media sites during working hours, unless authorised for specific business purposes.
- 5.8 Where employees bring their own personal mobile devices into the workplace, they must limit their use of these devices to official rest breaks, such as lunch-times. Allegations of over usage of personal mobile devices for personal reasons during core business hours will necessitate management attention.
- 5.9 Employees are advised to:
 - Familiarise themselves with this policy, the expectation of NHS Western Isles as an employer and their individual responsibilities as an employee.
 - Monitor the content of their social networking accounts, ensuring they comply with the policy standards. Ensure that any inappropriate information or material published on their networking pages or blogs, is removed immediately and measures put in place (where possible) to avoid any further re-occurrences (e.g. blocking certain individuals). NHS Western Isles reserves the right to contact the social media provider and request removal of materials in serious cases, including but not exclusive to cases which involve a likely risk of serious reputational damage to the employer or where there have been data protection breaches.

- Abide by professional codes of conduct (e.g. NMC, GMC, Code of Conduct for Healthcare Support Workers).
- Be aware of the Copyright 1988 Act and their individual responsibilities when posting/re-posting material (bearing in mind that copying a work protected by copyright on the web has just as serious consequences as doing so in 'real life').
- Consider not disclosing their profession and/or which organisation they work for in order to minimise any reputational risks and for their own personal safety. (N.B. this would not lessen responsibilities as an NHS Western Isles employee, and it may be the case that the individual can clearly be identified as an NHS Western Isles employee in another way – e.g. by accepting colleagues as 'friends' on a private account, or may be identifiable by the employer/colleagues by name/photograph and other information contained on their site – a potentially higher risk in a small community such as the Western Isles).
- Make it clear when publishing their opinions on-line, that these are their own personal views and that they do not represent the views of NHS Western Isles (if employees do disclose the name of their employer).
- Familiarise themselves with social media sites' privacy policies, settings and guidelines and pay particular attention to any posts/comments/pages that are public and could be seen and shared by anyone.
- Give consideration to the principles of the Once for Scotland Bullying & Harassment Policy in 2020..
- Check they know and trust the person when receiving online 'friend' requests and consider whether they wish to be associated with that person and the information and/or views that person publishes online before accepting the request.
- Consider whether they wish to be associated with information and/or views published on-line by a group or forum before accepting any request to join that group.
- If in doubt, do not 'like' share or comment on other content.
- Be aware that criminal sanctions can apply to the creation and dissemination of certain types of content on social media sites, just as they can elsewhere. Such content includes behaviour which:
 - Amounts to harassment and/or 'stalking'
 - Can be classed as obscene
 - Constitutes a public order offence

- Incites racial hatred
- Relates to or promotes terrorism
- Can constitute contempt of court
- Constitutes a communication which is 'grossly offensive' or of an 'indecent, obscene or menacing character' (section 127 of the Communications Act 2003). N.B. the offence is committed by sending the message. There is no requirement that any person sees the message or has been offended by it.
- Involves sending, or causing to be sent, a communication that is false, for the purpose of 'causing annoyance, inconvenience or needless anxiety to another'.

(The above list is not exhaustive)

(Staff should also be aware that people who pass on (e.g. re-post or share) messages can also be prosecuted when the original message is subject to prosecution).

6. Governance

- 6.1 NHS Western Isles will not routinely actively monitor staff members' social media accounts and does not intend to be overly prescriptive about how employees should conduct themselves in their private lives. Notwithstanding that, employees must be aware that, if a complaint or concern is made about a posting or comment (including appropriate evidence – e.g. a screenshot), NHS Western Isles will be obliged to consider the complaint/concern and take action where it is considered that there has potentially been a breach of Board policy. NHS Western Isles is also obliged to take action, in line with the Disciplinary Policy, if any postings deemed to be in breach of this policy (as described in section 4), are brought to the attention of/reported to the organisation in the absence of a formal complaint. Staff are reminded that any information posted on social media sites has the potential to become public, regardless of privacy settings.
- 6.2 All breaches or suspected breaches of this policy should be reported to line management. These will be investigated in accordance with NHS Western Isles policy as appropriate.

- 6.3 Some breaches of this policy may be considered to be so serious that they are deemed to constitute gross misconduct. Something considered to be gross misconduct could result in employee dismissal.
- 6.4 In the most serious of cases, the individual may be considered to have committed offences under civil or criminal law. In such cases, the employer would consider police involvement.
- 6.5 Should an employee find themselves the target of complaints, abuse, or bullying online they should consider removing the perpetrator(s) from their online 'friend'/'follower' list. Most sites also have mechanisms online which can be used to block the perpetrator(s) from initiating contact and also have mechanisms for reporting abuse online.
- 6.6 Should an employee find themselves targeted online by another NHS Western Isles employee, they should take a screenshot of any postings, report the matter to their line manager and consult the NHS Western Isles Dignity at Work Policy.
- 6.7 Where it is suspected that a breach has occurred whilst using NHS IT systems, including mobile computing or removable storage media, then the NHS Western Isles IT Security Policy/ Acceptable Use of IT Policy may also require to be consulted.
- 6.8 NHS Western Isles will, where necessary and legitimate, monitor/review activity from any of its workstations/devices.

7. Policy Review and Monitoring

- 7.1 This policy will be reviewed every two years, or sooner, if there is a requirement to respond to changes in technology/law/organisational structures/any other reason.

APPENDIX 1

NHS Western Isles – Email Etiquette

Every email sent by an NHS Western Isles member of staff creates a recorded profile of the sender and the organisation, therefore email correspondence must conform to NHS Western Isles Standards of Behaviour as well as professional Codes of Conduct (the Code of Conduct for Healthcare Support Workers applies to all staff who do not have a professional Code of Conduct).

Email should be used with care and consideration and, in the first instance, consideration should be given as to whether it is the best way to achieve an objective or communicate (for example a face to face meeting or discussion is more appropriate in situations where an ongoing conversation is required).

Emails should be concise, clear and respectful, with a clear indication included about whether a response or specific action is required from the recipient, and when the response is needed by.

Emails are the same in terms of information as all our communications – i.e. information should be shared on a 'need to know' basis only.

Prefixes – for internal emails

To assist staff, NHS Western Isles is introducing a prefix standard for the 'Subject Line' in certain internal emails. This will indicate the purpose of the correspondence and the expected response (or not) to help staff manage and prioritise emails.

The prefixes are listed below:

PREFIX	DESCRIPTION
ACT	Action required/for action
FOR INFO	For your information
REQ	Request
URG	Urgent – use judiciously, along with the '!' sign, giving consideration to the importance of the message for the person receiving the email. You should not use URG unless your message requires immediate action.
SOC	Social email to colleague(s)
[EOM] (suffix)	End of message – for example 'FOR INFO: Generator switch over at 3pm today EOM' saves recipient opening the full email.
STAFF BULLETIN	Used in emails to all mail users with information of general interest.

ADV	Adverts/vacancy information.
-----	------------------------------

Emailing with consideration

NHS Western Isles staff receive a high volume of emails on a daily basis and the volume of emails makes it difficult and sometimes frustrating for staff to prioritise the importance of messages.

The prefixes above will help staff to prioritise emails. Staff should also ensure that they only copy (cc) colleagues into emails appropriately. For example, do not copy senior members of staff into emails routinely, when communicating with colleagues. Senior staff should only be 'cc'd into emails in situations where the information is immediately relevant to them.

Particular care must also be taken when forwarding emails. It is essential that staff review the email trail/history to ensure that all the preceding content is appropriate to the new email recipient. A number of emails may contain sensitive or confidential information that should not be circulated beyond a specific group.

DO	DON'T
Do use the subject line to highlight email purpose and content.	Don't 'reply to all' without considering whether everyone requires a copy of the response.
Do keep emails short and concise.	Don't copy, send or forward anything that could be libellous, sensitive or offensive.
Do re-read your message before you send it, and use spell check.	Don't customise email format to an extent that it creates additional effort to read.
Do use the phone, or speak to people face to face if possible and where more appropriate (particularly when the information is required at short notice – e.g. late cancellation of meeting).	Don't use CAPITALS to write an email, this is seen as shouting.
Do take responsibility to let senders of routine emails know if you no longer require them.	Don't reply to an email when angry!
Do ensure, when sending large attachments, that they are only sent by email where necessary, as large attachments can block colleagues' mailboxes and cause frustration.	Don't send out an email if the wording or tone could be considered rude or offensive.
Do ensure that you keep distribution lists up to date.	Don't mark an email 'urgent' unless it is.

Do give some thought before attaching emails to emails.	Don't print off emails, unless necessary.
Do use common sense and respect for busy colleagues.	Don't send group emails unless appropriate – only send a group email when it's useful to all those receiving it.
Use a signature that contains job title and contact information. This ensures that people know who you are and how to get directly in touch with you.	Don't put in an email anything that you would not be comfortable with if it was made public – remember copies of emails can be requested under Subject Access Requests or Freedom of Information requests.
Do use the out of office facility. This is a requirement when staff go on Annual Leave.	Don't ask for an email to be issued to All Mail Users unless it complies with the All Mail Users Protocol for Information Distribution.
Do take personal responsibility for emails you send and receive.	

Email signatures

NHS Western Isles encourages the use of email signatures, mainly to ensure that people receiving your emails know who you are and how to contact you. Email signatures also present an opportunity to publicise or promote appropriate campaigns or projects (e.g. Living it Up logo, eMRec, Detect Cancer Early, etc).

For signatures, the following information should be included (bracketed items optional):

- Name
- Position
- Address
- Landline
- (Mobile)
- (appropriate corporate message or campaign logo)
- (NHS Western Isles Facebook and Twitter links/NHS Western Isles website link)
- (Gaelic translation of email signature is recommended)

Standard font should be used (Times New Roman, Arial or Garamond) in either black or dark blue.

(Please note that IT can assist with formatting. Outlook users will be able to create more complex signatures than web users.)

NHS Western Isles Communications Department	Contact Details
<p>Head of Communications, Claims and Patient Information, Maggie Jamieson</p> <p>Web Graphics and Media Specialists, Marissa MacLennan and Kerry Coleman</p>	<p>Tel: 01851 708060 Mob: 07810527457</p> <p>wi.coms@nhs.scot Maggie.jamieson@nhs.scot</p> <p>Marissa.maclennan@nhs.scot Kerry.coleman@nhs.scot</p>