POLICY ON CORPORATE USE OF SOCIAL MEDIA

Responsible Director:	Director of Corporate Communications
Approved by:	Corporate Management Team
Date approved:	July 2012
Date (s) Reviewed:	April 2014 January 2016
Date for Further Review	January 2020
Other relevant policies	Policy on Personal Use of Social Media Dignity at Work Policy on Stalking Internet Acceptable Use Policy Email Acceptable Use Policy Disciplinary Policy and Procedure Grievance Policy and Procedure

Agreed at Area Partnership Forum on 23 April 2014

CONTENTS

APPENDICES

1. Introduction

The term 'social media' refers to websites and networks where users have an opportunity to share photos, videos, opinions or even reviews and reports on their experience. Blogs, YouTube, Facebook and Twitter are all examples of social media.

There is growing evidence of the potential for social media to offer opportunities for our organisation to engage effectively with patients and communities.

The misuse of these social networks carries significant reputational, technical and legal risks and therefore this policy has been developed to provide clear advice and guidance to employees on the use of social media in a professional capacity.

The policy sets out a process for the limited and authorised use of social media for professional purposes to allow the organisation to realise the benefits of social media whilst ensuring the risks are appropriately assessed and managed.

Social media is a relatively new business tool and as is often the case with new business tools, there is a learning curve for any organisation that embraces it. NHSGGC recognises that the relationship of the organisation with social media will evolve and mature as our staff become more confident in its use and the opportunities it presents. The policy will therefore be kept under regular review.

This policy related to the professional use of social media within NHSGGC whether on a network PC or on an employee's own device.

It should be read in conjunction with the policy on personal use of social media**.**

Other relevant policies and legislation:

- Information Governance Policy
- Internet Acceptable Use Policy
- Email Acceptable Use Policy
- Information Technology Security Policy
- Freedom of Information Policy

- The Data Protection Act 1998
- The Computer misuse Act 1990
- The Copyright, Design and Patents Act 1988
- The Access to Health records Act 1990
- The RIP Act 2000
- The RIP(S) Act 2000
- Freedom of Information (Scotland) Act 2002
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Human Rights Act (1998)
- The Privacy and Electronic Communications (EC Directive) Regulations (2003)

2. Scope

This policy applies to all employees of NHSGGC, whether full-time or part-time, whether on permanent contracts, fixed-term or bank (as and when required) contracts.

It covers the professional use of social media within NHSGGC. It does not cover what you discuss, comment on or publish in your own time on your own personal profile. This is covered by the policy on personal use of social media.

3. Roles and responsibilities

NHS Greater Glasgow and Clyde will take all reasonable steps to ensure that employees are aware of this policy.

It is the responsibility of all staff using social media on behalf of NHSGGC to ensure they have read and understood this policy and ensure that they comply with all relevant legislation and associated policies.

The Corporate Communications Directorate has overall responsibility for identifying, monitoring and responding to all matters that can affect the reputation of the organisation. The Directorate should respond to any social media issue in the same way they would with any other media channel.

HI&T is responsible for information security and use both technology and process to ensure that IT systems perform as expected; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact the business of the organisation.

4. Personal conduct

Any information published online can be accessed around the world within seconds and will be publicly available for a long time. This makes it important to stick to the common principles shared across all forms of social media.

Any member of staff who is granted authorisation to use social media on behalf of the organisation must observe the following:

Be professional: Remember that you are an ambassador for NHSGGC. Be transparent and state that you work for NHSGGC. If you are writing about NHSGGC, use your real name, identify that you work for the organisation and be clear about your role.

Be connected: If you have been authorised to create an official NHSGGC or NHSGGC-related project social media site or DVD for posting on YouTube or similar activity, the Corporate Communications Directorate will give you an approved logo, guidance and ensure that you coordinate with other NHSGGC web/social media sites.

Perception is reality: In online social networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as an NHSGGC employee, you are creating perceptions about your expertise and about NHSGGC among our stakeholders, clients and general public as well as your manager(s) and colleagues. Be sure that all content associated with you is consistent with your work and with the NHSGGC values, priorities and professional standards.

Be credible: Be accurate, fair and thorough. Correct your mistakes and do not alter previous posts without indicating that you have done so. Whenever possible, ask a colleague or your

manager to review your postings. This will reduce the number of errors in typing or wording and should also help mitigate against posting incorrect or inappropriate information.

Be aware: Always remember that participation online results in your comments being permanently available and open to be republished in other online and traditional media (print and broadcast). Remember that journalists regularly track Facebook, Twitter, YouTube and LinkedIn and the whole range of social media.

Be safe: Never give out personal details such as home address and phone numbers or other sensitive or confidential information. Do not give undertakings of privacy or confidentiality that the organisation cannot meet. Make sure that contributors are aware that they are not using a secure space. Do not use individual work email accounts when setting up an account but a generic project email address. Follow NHSGGC's policy on safe password practice to minimise risks of security breaches e.g. change the password or a regular basis; do not use an obvious (e.g. QWERTY) password.

Be legal: Stay within the legal framework and be aware that discrimination, libel, defamation, copyright, Freedom of Information and data protection laws apply as well as fair use and financial disclosure laws. A defamatory comment is one that is capable of damaging the reputation of an individual or organisation. If successfully sued, you could be liable for costs and damages. Defamation laws also apply to businesses.

Be aware: Intellectual property claims of social media service providers vary widely. Where providers claim "ownership" of content created on or added to the site, consider whether it is appropriate to proceed.

Follow the site's Code of Ethics: There are numerous codes of ethics for bloggers and other active participants in social media, all of which will help you participate responsibly online.

Be alert: You should also monitor social media for discussion about NHSGGC, your specific project/campaigns or the products/services you deliver. Capture records as appropriate. If the use of social media has been authorised for consultation or discussion to inform decisions, appropriate records of the content must be captured and held on NHSGGC systems as part of the audit trail for that decision.

Show respect: Avoid discriminatory, insensitive language or obscenity and do not engage in any conduct that would not be acceptable in the workplace. Do not write posts that are abusive, threatening, harmful, obscene, profane, sexually suggestive, racist, homophobic, sexist or that incite hatred against any group.

Respect privacy: Do not cite or reference NHSGGC staff, stakeholders, or contractors without their approval. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory. No personal identifiable data should be published without the consent of the individual.

Be clear: about the status of content. Make clear that any document or data on a NHSGGC-initiated or administered forum is considered to be held on behalf of NHSGGC for the purposes of the Freedom of Information (Scotland) Act 2002 and may be disclosed in response to requests.

Removal of postings: Whenever removing postings a copy should be kept. The copy may be required in the event of a complaint about the moderation of the site. When correcting errors about NHSGGC or an NHSGGC piece of work, be transparent about who you are. Never remove criticism of NHSGGC. Instead, respond to legitimate criticisms in a measured and accurate way. Remember to advise your Line Manager.

All staff have a responsibility to ensure compliance with relevant NHSGGC polices including the Code of Conduct, Data Protection, Freedom of Information, Bullying and Harassment and patient confidentiality.

5. Use of social media for business purposes

(i) Procedure for approving use for business purposes

The policy of NHSGGC is that social media can only be used for business purposes if authorised. General access to social networking sites is not permitted on the NHSGGC network and access to these sites will be blocked unless authorisation is granted.

The purposes to which social media can be used for interaction with the wider public are vast so NHSGGC will focus on a first wave of applications which are relatively low risk from security/compliance perspective, create maximum impact from relatively little outlay and support and can be used as a launch pad for more ambitious usage of social media in the future.

Applications of social media use may be made for the following business purposes:

(i) Business continuity communications
(ii) News and announcements
(iii) Public education/health campaigns
(iv) Understanding and monitoring public opinion, including engagement and consultation
(v) Networking with patient support groups

(See Appendix A, Section 7 for examples of good practice for each of these first wave applications).

Social media must not be used for knowledge management purposes. There are existing internal resources within NHSGGC for staff to share information, documentation and expertise.

Any individuals or team wishing to apply to use social media for professional purposes which fit within the scope of (i) to (v) above must complete the attached risk assessment form (Appendix B) and business case (Appendix C) and submit these via their line manager to the Corporate Communications Directorate.

The Corporate Communications Directorate will consult with the relevant Director or Head of Service and with the Director of HI&T to reach a decision on whether to approve the application for use.

The business case must describe which social networking site is involved, the nature of the NHSGGC project, the purpose of the presence on the social networking site, how this will be resourced, managed, monitored and evaluated, how you plan to interact and deal with queries, the training requirements, how the information on the site will be monitored and stored for Freedom of Information purposes and the exit strategy.

You must not disclose information, make commitments or engage in activities on social media on behalf of NHSGGC unless you are authorised to do so. This authority will normally be explicitly granted to named individuals but may be delegated depending on individual circumstances. Any member of staff granted permission to use social media must complete the acceptable use certificate (Appendix D) and send it to their HR Department with a copy to the Directorate of HI&T.
Any individual who is authorised to use social media must at all times ensure compliance with relevant legislation and NHSGGC policies including patient confidentiality, data protection, Freedom of Information, financial disclosure and copyright.

You must have a plan in place to monitor and capture the content of any social media that you use so that it can be held on NHSGGC systems as part of an information governance audit trail to

ensure that the content is not inappropriately omitted from the records of an activity or missed from research or disclosure, e.g. from an FOI request. This is particularly important if the SNS is used for engagement and consultation as it will form part of the evidence base for decision making.

Authorised NHSGGC activity will normally conform to a consistent style and branding. For instance, the default position will be that all accounts should be harmonised; i.e., every Twitter account would start with @nhsggc." Appendix A contains the recommended procedure for creating accounts and profiles, along with corporate images for social networking environments. The appendix also lists the most commonly used social media utilities, their various uses and the purpose of each site, recommendations for an appropriate and productive presence and the criteria for finding the best communicative style for each tool.

Staff responsible for monitoring and updating social networking sites will carry out regular evaluations to report on the usage of the site, interaction of friends/group members, number of friends/members, what has been uploaded to the site in the period since the last evaluation and any incidents relating to cyber bullying, inappropriate posts or inappropriate member/follower requests (see Appendix E for Standard Reporting Form). If there have been any incidents the evaluation report will include any incident reports that were completed and what action was carried out to resolve the incident and if anything has been put in place to prevent it from recurring.

Each social networking site has its own measurements and tools (such as Facebook Insights) and these should be used to generate the statistics.

The evaluation report will be used to decide if the use of a social networking site has been successful and beneficial to the project. If the evaluation reports are not favourable (e.g. repeated incidents, no postings, membership decreasing) the decision may be made to disband the site and no longer use it in relation to the project.

NHSGGC reserves the right to request the certain subjects are avoided, withdraw certain posts, and remove inappropriate comments.

(ii) Responding to comments/postings on social network sites

As a publicly accountable organisation with more than one million patient contacts every year, NHSGGC accepts that our organisation and staff will be the subject of comment and opinion on social networking sites. The Corporate Communications Directorate will monitor social media and agree with colleagues when it is right to respond to these comments about our staff and services. This may include an investigation into the issues being reported, if appropriate.

There may be instances where video or commentary is posted that goes beyond legitimate, acceptable opinion e.g. a breach of patient confidentiality or a defamatory comment about our staff.

If you become aware of any instance of inappropriate comments or video of our patients or staff on any social media or website, you should report this to the Corporate Communications Directorate.

The Directorate will liaise with appropriate directorate leads, our Caldicott Guardian, the patient involved or his/her relatives and, if appropriate, the Central Legal Office to agree a response, including requesting the deletion of the comment or video if necessary.

(iii) Freedom of Information

NHSGGC has a legal obligation to comply with the requirements of the Freedom of Information (Scotland) Act 2002 under which a person or organisation is entitled to request information from a public body. NHSGGC has established systems in place to handle FOI requests and has created dedicated email address through which requests for information can be submitted. However it is

still possible that NHSGGC accounts created on social networking sites might be seen as a route through which FOI requests could be submitted.

Staff responsible for monitoring social networking sites should therefore be alert to this possibility and should ensure that the content of all communications sent to NHSGGC through social networking sites are screened to establish whether they constitute a valid request for information and appropriate action taken if necessary. (A valid request must state the name of the applicant and an address for correspondence. It must also describe the information being requested.) Further information on FOI can be accessed through the Board's Freedom of Information Manager, or relevant Head of Administration.

6. Governance

All breaches or suspected breaches of this policy must be reported to and investigated appropriately by management in accordance with NHS Greater Glasgow and Clyde Disciplinary Policy and Procedure. Where it is suspected that a breach has occurred whilst using NHS IT systems, including mobile computing or removable storage media, then the NHSGGC IT Security Policy, NHSGGC Internet Acceptable Use Policy, NHSGGC Mobile Devices, Data Breach Policy and Media Policy should also be consulted. Advice should also be sought from Human Resources.

Should there be evidence to suggest that an employee has not adhered to the standards set out within this policy, then disciplinary action may be taken against them in accordance with the NHS Greater Glasgow and Clyde Disciplinary Policy and Procedure. In certain circumstances this may lead to termination of the contract of employment and/or legal action taken against the individual.

7. Review of policy

Due to the pace of development of social media, this policy will be reviewed every six months unless the introduction of any new or amended relevant legislation or changes to the security structure of any social networking site warrants earlier review.

8. Communication and implementation

Staff authorised to use social networking sites will be trained. Peer group training is available in the short term and a closed SharePoint site has been established for the sharing of best practice.

The policy will be communicated via StaffNet and the other internal communications tools and through the Information Governance and IT Security Framework.

1) Social media defined

Social media is a term used to refer to online technologies and practices that are used to share opinions and information, promote discussion and build relationships.

Social media services and tools involve a combination of technology, telecommunications and some kind of social interaction. They can use a variety of different formats, including text, pictures, video and audio clips.

New tools are being created all the time. They include mass-user social networking, personal blogs and professional communities collaborating on wikis, forums and new uses of video communications.

Using social media in itself does not make for good practice. In order to be effective, initiatives must form part of a wider communications strategy and bring at least some of the benefits listed below.

2) Benefits, challenges and limitations

Good use of social media can help us better understand, respond to and attract the attention of specific audiences. It enables two-way communication with people in the places where they are already engaging with their interests.

Social media can:

- Increase access to audiences and improve accessibility of communication
- Enable us to be more active in our relationships with partners and stakeholders
- Offer greater scope to adjust or refocus communications quickly, where necessary
- Improve the long-term cost effectiveness of communications
- Increase the speed of feedback and input
- Reach specific audiences on specific issues
- Engage with specific 'virtual' communities
- Reduce our dependence on traditional media channels

Challenges and limitations

- No social media sites are fully secure. Be conscious that any content placed on them may be seen by people other than the intended audience and must be considered as public.
- Managing reputation in a setting which is meant to encourage discussion and comments needs careful consideration.
- There are significant resource implications in terms of managing and responding to comments and online discussion.
- Social media is not generally backed up in the same way as internally networked services.
- Robust information governance is needed to ensure that content created on social media is not inappropriately omitted from the records of an activity or missed from research or disclosure, e.g. from an FOI request

3) Protocols for specific networking sites

Facebook

This social network provides a platform to communicate and share information, photos, videos and links with users we know. Users can also participate in communities that may interest them. Facebook also allows us to send private messages to their contacts (known as friends) and to other users who we may not know but who are on Facebook, and to create events and invite others to join.

Facebook is one of the most popular social networks worldwide and one of the largest in terms of active users. This makes it an appropriate platform to convey information to a broad audience.

Facebook offers several options depending on whether users represent themselves, an institution, a company, or a group of people. Thus a prolife, a page (official or community page) or a group can be created depending on the purpose within this social network.

Pages are designed for institutions and can be managed by one or several profiles (users). Creating a profile for a department or service is not an option because it would break Facebook's terms of use.

One of the main features of Facebook pages is that they do not have a list of friends, as profiles do, but they have fans.

Integrating Facebook in other sites can be achieved in several ways:

- In our own website www.nhsggc.org.uk
- Third-party sites

Images uploaded must comply with corporate identify guidelines (insert photolibrary guidelines) and be fully consented for publication.

If approval is given to set up a Facebook page, the Corporate Communications Directorate will provide you with graphic elements to confirm the official nature of the account and agree a page name with you.

Named individuals will have responsibility for the account. These individuals should use a generic email account rather than their own individual work email account when establishing a Facebook page.

Examples of corporate images for Facebook

Privacy settings on Facebook should be applied as follows:

- Photo Albums – Photo albums will only be able to be viewed by fans or group members. Only fans/group members can comment on pictures.

- Published Application Stories – No application will be subscribed to; this will prevent automatic wall stories being published to the profile by the application.

- Contact Information – Contact information, in the form of an email address, will be publicly available to allow people interested in the group/project to contact staff before becoming a friend/member of the SNS profile.

- Wall Posts – Wall posts will be publicly available to enable those interested in the group/project to view what is being discussed, but only friends/members can post comments to the wall.

- Friends/Members Lists – Friends/Members lists will be kept private, only other friends/members will be able to view the friends/members list. This is as private as they can be made, at the moment there is no option to make friends/members lists completely private from everyone.

- Login Notifications – Login notifications are an opt-in security feature that sends alerts when your account is being accessed. If you receive a login notification and the login was not made by you, you will find instructions in the email or text alert on how to reset your password in order to secure your account from being compromised. Approved devices can be named and saved (e.g. home computer and work computer) and notifications will be received when the account accessed from a computer that is not an approved device. Text message approvals can also be set up which will send a code via text to a registered mobile number when the profile is logged into from an unrecognised computer/device.

A Facebook account which has not been updated for six months is considered inactive and can be removed automatically.

Twitter

Twitter is a micoblogging service for publishing short text messages (up to 140 characters). As a Twitter user you can post updates, follow and view updates from other users (this is akin to

subscribing to a blog's RSS feed), and send a public reply or private direct message to connect with another Twitterer.

Though users can answer the prompt, "What are you doing?", tweets have evolved to more than everyday experiences, and take the shape of shared links to interesting content on the web, conversations around hot topics (using hashtags), photos, videos, music, and, most importantly, real-time accounts from people who are in the midst of a newsworthy event, crisis, or natural disaster.

Twitter is a great tool to inform about new services to provide reference information and to cover live events, but it is also a tool for user discussion and collaboration.

If you are considering a Twitter account the three most important questions to consider are:

- Who are the people we want to reach? This is important to establish before you create an account because you may need more than one account.
- Will Your Tweets be interactive? Will you allow people to comment back? Or just get updates? Will your subscriber list be public or private?
- Who Will Monitor the Account? Decide who will Tweet and what they will Tweet.

If approval is given to set up a Twitter account, the Corporate Communications Directorate will provide you with the graphic elements to confirm the official nature of the account and agree an account name with you. Each account must be associated with a different email address because Twitter does not allow associating multiple profiles to the same email address.

Named individuals will have responsibility for the account. These individuals should use a generic email account rather than their own individual work email account when establishing a Twitter account.

Tips to increasing Twitter followers:

- Align your tweets with your purpose;

- Add value – it's important to add value in your tweets such as by the use of links. Content must be carefully read before being linked and the source needs to be reliable;

- Include buzzwords and #hashtags ask yourself what types of keywords your desired audience will search for then make sure you include those types of buzzwords in some of your tweets. Make sure that if you are tweeting about a topic that has a hashtag that you include the hashtag at the end of your post. A hashtag is simply a word or phrase that is associated with a specific topic that people are following on twitter. You can visit hashtag.org to find the different topics. To make up your own hashtag simply check to see if it already is used for a different topic and, if not, include it at the end of your related tweet.

Twitter accounts can be integrated in other spaces by means of small applications (widgets) that embed external information in a website to promote. These widgets can be used on:

- Our own website – www.nhsggc.org.uk
- Our own external sites e.g., Facebook pages by means of a tab, a sidebar widget of via automatic publications
- Third party sites

Examples of corporate images for Twitter

Privacy settings on Twitter:

- Followers – When someone starts to follow you on Twitter, they can automatically see your Tweets. There is a function to approve followers first, to do this you should check the box 'Protect my Tweets' in the Account section of Settings. This means that only people who are following you will be able to see your Tweets and they will not be posted to the public section of the website. An email is sent when a new person requests to follow you. Email notifications can be set up in the notices section of Settings.

- If you have protected your tweets, your Twitter feed cannot be linked to any websites (some websites have their Twitter feed linked directly to their home page to enable people who are not on Twitter to see what they are tweeting about).

- Tweets – Tweets can either be publicly available, which means that they will appear on the timelines of your followers and also the Twitter public timeline, which shows everyone accessing the site what is being tweeted about at that time. Leaving your tweets public means that more people can see what you are tweeting and may decide to follow you and you can also link your tweets to the website associated with your group/project.

- Profile Information – Your profile information (username, location, web page (if entered) and bio) are all publicly available and there is no option to keep this information private. Information here should be kept to what is already publicly available, e.g. what the group/project is for and where they operate.

A Twitter account which has not been updated for six months is considered inactive and can be removed automatically.

YouTube

YouTube is a platform which allows users to publish, watch and share user-generated videos. YouTube is ideal for disseminating informative or educational audiovisual materials about our activities or health issues.

YouTube allows personalisation of accounts. There are some differences between basic accounts, on which only videos of ten minutes of less can be uploaded, and premium accounts that have no length restrictions.

- Basic accounts: the avatar and the basic colours of the channel can be personalised
- Premium accounts: the avatar, basic colours of the channel can be personalised and a header of 960px width and 150px height can be published.

YouTube channels require authorisation and once approved, the person responsible will be given an appropriate avatar and instructions on use of corporate image. Named individuals will have responsibility for the account.

Videos uploaded must comply with corporate identify guidelines and be fully consented for publication.

It is not recommended to link YouTube account with those of Facebook and Twitter. It is preferable to manually control the circulation of videos on other social networks.

At the time of publishing a video it is necessary to give it a title and provide a brief description. It is also best to complete the *Tags* field with keywords in order to make the video easier to search for.

Flickr

Flickr is an online photo management and sharing application. The free version has a monthly upload limit of 100 MB (10MB) be image; user with grater uploading requirement will need to upgrade to the pro version.

Flickr also enables the publication of short videos (90 seconds).

Flickr allows users to choose their own avatar. Image size is 48 x 48 px.

Flickr accounts will require authorisation and once approved, the person responsible will be provided with an appropriate avatar and instructions in respect of the individual account and corporate image. Named individuals will have responsibility for the account.

Images uploaded must comply with corporate identify guidelines and be fully consented for publication (see below).

The Flickr account should be configured to that it only works as an image bank. To avoid the publication of comments that would make it a social network go to Privacy and permissions, then to preferences for new uploads/who can add notes, tags and people, and select Only you.

4) Comments protocol

Each site must have a policy regarding the acceptability of information added to it and the basis for moderation of the site.

The remainder of this section is to be added to all social networking sites:

We welcome you and your comments to this page. The purpose of this page is to present matters of public interest and updates on the activity of the service/group. We encourage you to submit your questions, comments and concerns, but please note this is a moderated online discussion and information site and not a public forum. Please also be aware that anything that you write will be visible to everyone who accesses this page.

Requests for information under the Freedom of Information (Scotland) act 2002 or the Environmental Information (Scotland) Regulations 2004 should be submitted through our email address at: foi@ggc.scot.nhs.uk, or visit the NHSGGC Freedom of Information microsite www.nhsggc.scot.nhs.uk/foi for further details.

This site is moderated on Monday to Friday intermittently between the hours of 09:00 and 17:00, but excluding public holidays.(This sentence should be altered to suit the planned moderation hours)

Once posted, the moderators reserve the right to delete submissions that contain vulgar language, personal attacks of any kind or offensive comments that target or disparage any ethnic, racial or religious group. Further to this, we also reserve the right to delete any comments that:

- *are spam or include links to other sites*
- *are clearly off topic*

- *advocate illegal activity*
- *promote particular services, products or political organisations*
- *infringe on copyrights or trademarks*
- *use personally identifiable medical information (We recommend you not share any of your medical information on our Social Networking pages)*
- *contain case-specific and other confidential information*

NHSGGC do not take any responsibility for people making contact with members via this profile's friends list. Whilst every precaution has been taken to ensure the privacy of the friends list, it is up to the individual to control their own privacy settings and who can view their profile.

*Please note that the comments expressed on the site do not reflect the opinions and position of NHS Greater Glasgow and Clyde or its offices and employees. If you have any questions concerning the operation of this online moderated discussion and information site, please contact email _____ (*Note, this is to be a generic mailbox which is accessible to the individual(s) moderating the SNS*).*

5) Photography/video protocol

If you want to publish photographs/videos on social media, you must have the legal rights to do so. All images to be used should therefore be either Crown Copyright or have the permission of the owner of the photograph/video to publish on social media.

Every person who features in the photography/video must have agreed to have his or her photo published online and completed a written consent form to confirm consent. Please note that all images on the NHS Scotland Photolibrary www.nhsscotlandphotolibrary.org come with this consent.

All images used should aim to portray real life in NHS Scotland and should depict an honest, positive image of a modern and diverse organisation. Images should show realistic situations, with premises, equipment and dress arranged in accordance with current policies/best practice. Care must be taken to conform to the current dress code and uniform policies for NHS staff, for example, picture showing doctors in white coats with stethoscopes round their necks must not be used.

6) Malware

Usage of online social networks significantly increases the likelihood of malware (such as viruses, Trojans and worms) being imported into NHS networks even where robust anti-virus measures are in place. Anti-virus software is run on all NHS GGC computers however threats exist on social networking sites that NHS GGC does not have technical controls to mitigate.

Users must:

- Use a strong, hard to guess password on the SNS
- Be extremely cautious in following links posted by members of the public
- Be extremely carefully if formatted text appears as a posting it could represent malware.
- Never install an executable programme
- Beware of phishing attacks – questions that may cause you compromise some personal information
- Check that information that you have posted has not been altered without your approval – web sites are often compromised and a malicious person may have changed your postings.

7) Examples of first wave applications of online social networks[1]

Business continuity communications

Online social networks (OSNs) can be used to get key messages out quickly to a wide audience during emergencies. The winter of 2010/11 in Scotland was the worst for 40 years leading to the closure of public buildings and schools. Some NHS boards used Twitter micro-blogs or announcements on Facebook to inform the public about the availability of services. Traditional channels (such as bulk emails, telephone calls or updating front web pages) are not always option if there is a disaster and IT systems are down. Micro-blogging could also be used to connect with employees as part of continuity plan.

Using OSNs in this way is also a good way of getting 'followers'. Most citizens may follow NHS tweets for the first time during bad weather but can be encouraged to maintain contact afterwards provided tweets remain relevant (e.g. for significant virus outbreaks rather than an avalanche of routine updates on services).

The health organisation can also monitor reaction and feedback contained in messages/tweets in order to gauge the effectiveness of its emergency response (e.g. customers suggesting that a road that provides access to a hospital is now open or complaints). Some boards are Twitter 'followers' of public organisations such as the Meteorological Office which enables them to aggregate and then condense lots of news-feeds relevant to their own audience.

News and announcements

Boards can upload subtly different news and announcements onto OSNs than mainstream channels such as official web-sites. NHS Lothian have used Twitter to show when the minor injuries clinic might be more appropriate for some cases than Accident and Emergency. This not only informs the public but can potentially help boards to free up resources by funnelling patients to the best place.

The more informal nature of OSNs means that boards can put announcements which would not normally make the front page of an official health board web-site (such as health charity and other community events) but which foster good relations and 'social presence'. The viral nature of OSNs means that word can get around more quickly than other channels (companies call it 'guerrilla marketing').

Understanding and monitoring public opinion

The fundamental difference between normal e-communications via official web-sites and OSNs is that the 'funnel is reversed': i.e. more communications are coming in than going out. Each official health-related 'tweet', video-clip or news item on Facebook will generate far more of response than was the case with traditional web feed-back forms.

- **Correcting factual inaccuracies**

It is not the place for officials to enter into public debates. But there are cases where OSN conversation strings highlight straightforward inaccuracies (or even myths). Virtually all of the discussion boards relating to eCare for example repeated falsehoods (e.g. that this was a state database on children by the back door). Such misunderstanding on influential sites such as Netmums (which has 1m+ members) can seriously impair the ability of health bodies to roll out and get public acceptance of new tools and services. A news story which aims to correct a myth can be placed into OSN fora as part of an overall communications plan. Alternatively, there could be a 'hot seat' session where for a limited time-slot a senior official (or minister) might host a question

[1] Source: Online Social Networking Guidance, eHealth, Scottish Government. October 2011

and answer session. This is safer than entering into conversation strings already initiated by citizens (i.e. could be construed as state interference or even political opinion shaping).

- **Straw-poll canvassing**

The uncontrolled and anonymous nature of OSNs, mean that they cannot as yet really replace formal public consultations and statistical analysis. But OSNs can offer a quick and easy way to 'test the water' before making significant investment in new services or creating new policies.

Sites such as Patient Opinion and dash-boards on hospital Facebook sites are already collecting patient experiences. The Patients Rights (Scotland) Act 2011 specifies that NHS bodies should "encourage patients to give feedback or comments, or raise concerns or complaints, on health care".

Public education and health campaigns

OSNs can be incorporated into wider public health campaigns. 'Tweet what you eat' (healthier eating), 'quitter twitter' (give up smoking), 'helping those, helping others' (Blood Donation) are just some of the blogs/discussion fora set up by boards. The advantage of OSN here is that the official content is mixed in with tips and self-help sent in by the public. The informal and less censorious tone can be more accessible than some poster/web-site campaigns.

Patient support groups

There has been an explosion of interest in 'medical support sites'. More than two thirds of all health-related searches start at search engines (e.g. Google a health condition in order to find a support group). The quality varies enormously from respected charities to commercial companies (basically marketing tools dressed up as OSN) to sites set up by one individual on a kitchen table.

NHS Scotland already provides high quality advice (e.g. NHS Inform) and sign-posts to support groups. On the whole it does not make practical sense for the NHS to compete with or duplicate these existing groups. Many have grown up over many years and have a strong brand. The question instead is how far the NHS should actively engage with any of these existing OSNs by sponsorship, providing content and two-way interaction. If OSNs are chosen carefully there are many mutual benefits: members of the OSN can be informed about new health services in a given area (e.g. via post-code) and links can be placed to comprehensive advice on official web-site.

Corporate Use of Social Media Policy

Application process/forms
Any individuals or team wishing to apply to use social media for professional purposes which fit within the scope of the Corporate Use of Social Media Policy must complete the attached risk assessment form (Appendix B) and Business case (Appendix C) and submit these via their line manager to the Corporate Communications Directorate by email to: margaret.brodie@ggc.scot.nhs.uk

The Corporate Communications Directorate will consult with the relevant Director or Head of Service and with the Director of HI&T to reach a decision on whether to approve the application for use.

NHS Greater Glasgow and Clyde

ID:

Risk Assessment Form

Use this form for any detailed risk assessment unless a specific form is provided. Refer to your Summary of Hazards/Risks and complete forms as required, including those that are adequately controlled but could be serious in the absence of active management. The Action Plan and reply section is to help you pursue those requiring action.

Name of Assessor:	Assessor Name	**Post Held:**	Assessor's Post
Department:	Assessor's Department	**Date:**	Date of Risk Assessment
Subject of Assessment: E.g.: hazard, task, equipment, location, people			
Hazards (Describe the harmful agent(s) and the adverse consequences they could cause)			
Description of Risk Describe the work that causes exposure to the hazard, and the relevant circumstances. Who is at risk? Highlight significant factors: what makes the risk more or less serious – e.g.: the time taken, how often the work is done, who does it, the work environment, anything else relevant.			
This section will only contain risks that are ***additional*** to those shown in the general risk assessment. Examples would include patient harm from delayed response for cases such as mental health issues or an increased level of risk related to medical advice (as apposed to healthy living advice) being provided using SNS. All additional risks should be provided.			

Existing Precautions

Summarise current controls In place	**Describe how they might fail to prevent adverse outcomes.**

The risks declared above have been assessed as

Likelihood		**Impact/Consequences**	
Almost Certain		Negligible	
Likely		Minor	
Possible		Moderate	
Unlikely		Major	
Rare		Extreme	

Level of Risk - Is the control of this risk adequate?
Give more than one risk level if the assessment covers a range of circumstances. You can use the 'matrix' to show how 'likelihood' and 'consequences' combine to give a conclusion. Also, be critical of existing measures: if you can think how they might fail, or how they could be improved, these are indications of a red or orange risk.

Risk Matrix

Likelihood	Impact/Consequences				
	Negligible	Minor	Moderate	Major	Extreme
Almost Certain	Medium	High	High	V High	V High
Likely	Medium	Medium	High	High	V High
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Medium	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

Very High **High** **Medium** **Low**

Current risk level

Given the current precautions, and how effective and reliable they are, what is the current level of risk? **Green** is the target – you have thought it through critically and you have no serious worries. Devise ways of making the risk green wherever you can. **Yellow** is acceptable but with some reservations. You can achieve these levels by reducing the inherent risk and or by effective and reliable precautions.
High (Orange) or Very High (Red) risks are unacceptable and must be acted on: use the Action Plan section to summarise and communicate the problems and actions required.

Action Plan (if risk level is High (Orange) or Very High (Red)

Use this part of the form for risks that require action. Use it to communicate, with your Line Manager or Risk Coordinator or others if required. If using a copy of this form to notify others, they should reply on the form and return to you. Check that you do receive replies.
Describe the measures required to make the work safe. Include hardware – engineering controls, and procedures. Say what you intend to change. If proposed actions are out with your remit, identify them on the plan below but do not say who or by when; leave this to the manager with the authority to decide this and allocate the resources required.

Proposed actions to control the problem List the actions required. If action by others is required, you must send them a copy	By Whom	Start date	Action due date

Action by Others Required - Complete as appropriate: (please tick or enter YES, name and date where appropriate)

Report up management chain for action	
Report to Estates for action	
Contact advisers/specialists	
Alert your staff to problem, new working practice, interim solutions, etc	

Reply

If you receive this form as a manager from someone in your department, you must decide how the risk is to be managed. Update the action plan and reply with a copy to others who need to know. If appropriate, you should note additions to the Directorate / Service Risk Register.

If you receive this as an adviser or other specialist, reply to the sender and investigate further as required.

Assessment completed - date:	**Review date:**

Project Business Case

Project Name			
Directorate		Project Sponsor	
Project Description			
Social Network (s) to be used			
Purpose of the presence on social networking site			
How will presence be resourced? (e.g. IT access, staff to be allocated)			
Designated staff who require access	Name	Current approval	Training required
		Y/N	Y/N
		Y/N	Y/N
		Y/N	Y/N
		Y/N	Y/N
Risk Assessment provided	Yes / No		
Frequency at which the social network site will be moderated/updated			
Plan to interact and deal with queries			
Information storage arrangements			
Exit strategy			
Approval: Yes / No	Signed:…….. Designation:……..		

Appendix D

Acceptable Use Certificate

Staff Declaration Form

Internet Social Networking Policy - DECLARATION

I confirm that I have read and understood the Internet Social Networking Policy, and accept that my usage of Internet Social Networking sites will be audited and monitored. I agree to using Internet Social Networking Sites (SNS) for NHSGGC work purposes only and will not access my personal Social Networking profiles at any time from a work computer.

I agree to the following points:
I will not leave my computer unattended while logged into any SNS
I will only access SNS from my own NHS computer (except in the case of a technical failure of that PC)
I will not keep a written note of the log in details for any SNS in a visible place
I will not give out the log in details for any SNS to anyone who is not authorised to access SNS on NHS computers
I will inform IT and HR if I leave my current post for another NHS post or if my current post changes and I no longer require access to SNS for work purposes
I will report regularly on the interaction that has taken place on the SNS to my line manager & the IT department
I will report any incidents of inappropriate posts/behaviour on any SNS to my line manager immediately and remove them from the site
I will ensure that the privacy settings on SNS profiles are set to those described in the Internet Social Networking Policy
I will not access any SNS for personal reasons
I will not allow other members of staff to access their own personal SNS on my work computer.

I understand that failure to comply with this will result in my access to Internet Social Networking Sites being revoked and also may result in disciplinary proceedings.

Internet Social Networking Sites will only be accessed from the below mentioned computer and not from any other NHS PC, laptop or mobile device.

Employee Name……..

Employee UserID……...

Employee Signature……

Line Manager Name……

Line Manager Signature……..

Date……

Please return the signed original of this form to the HR department where it will be retained in your personnel file. **A copy must also be sent to the IT department**.

Take and retain a photocopy for your own reference purposes.

Standard Reporting Template

Project Name	
Project go live date	
Facebook Statistics	(If not using Facebook enter N/A)
Total number of postings	
Number of postings by project team this month	
Number of responses this month	
Total number of Likes	
New likes this month	
Significant feedback	
Note: Facebook insights data should be submitted with this form	
Twitter Statistics	(If not using Twitter enter N/A)
Total number of Tweets	
Number of Tweets by project team this month	
Number of responses this month	
Total number of Followers	
New followers this month	
Significant feedback	
YouTube Statistics	(If not using YouTube enter N/A)
Total number of views	
Change this month	
Significant feedback	
Any Incidents	Incident description including the network on which it occurred, impact and actions to prevent any recurrence.