

<b>Title:</b>				
<b>SOCIAL MEDIA POLICY</b>				
<b>Date Approved</b>	<b>Approved by:</b>	<b>Date of review:</b>	<b>Policy Ref:</b>	<b>Issue:</b>
January 2016	JSPF	January 2018		1
<b>Division/Department:</b>		<b>Policy Category:</b>		
Human Resources / Communications / Nottinghamshire Health Informatics Services		Corporate Governance		
<b>Author (post-holder):</b>		<b>Sponsor (Director):</b>		
Information Governance Manager / HR / Communications		Director of NHIS Executive Director of HR		

## CONTENT

SECTION	DESCRIPTION	PAGE
1	Introduction	3
2	Policy Statement	3
3	Definitions	4
4	Role and Responsibilities	5
5	Scope of Policy	5
6	Consultation	5
7	Duties & Responsibilities – Private Use of Social Media	5
8	Duties & Responsibilities – Trust Use of Social Media	7
9	Reporting Inappropriate Behaviour on Social Media	7
10	Evidence Base	7
11	Monitoring Compliance	7
12	Training Requirements	7
13	Distribution	8

14	Communication	8
15	Author and Review Details	8
16	Appendices - diagrams, flow charts, evidence	9

The issue of this page is the overall issue of this procedure.

The current issue of individual pages are as follows:

<b>PAGE</b>	1	2	3	4	5	6	7	8	9	10	11
<b>ISSUE</b>	1	1	1	1	1	1	1	1	1	1	1
<b>DATE</b>	01/16	01/16	01/16	01/16	01/16	01/16	01/16	01/16	01/16	01/16	01/16

## **1 INTRODUCTION**

- 1.1 The world of communication is changing and Sherwood Forest Hospitals NHS Foundation Trust (the Trust) aims to be a dynamic organisation embracing new technologies and ways of working. The rise of social media is changing the way we, and every organisation in the world conducts its business. Millions of people use social media everyday responsibly and it is becoming an increasingly important communications tool.
- 1.2 The Trust is making increased use of social networks to engage with their patients, service users and other stakeholders, and to deliver key messages for good healthcare and services generally. Online digital communications are used by the Trust's communications department to further extend its interactions with patients, service users and other stakeholders and their use is likely to be further extended as new communications channels become available.
- 1.3 There is a large range of social media platforms available, such as Facebook, LinkedIn and Twitter. Many staff use these in their own time, using their own computers and smartphones. In addition to personal use, for many, this is an important channel for professional communication, for learning and gaining a work profile.
- 1.4 This policy is necessary as many employees enjoy sharing their knowledge, learning and experience with others of similar roles and interests. The Trust acknowledges these online activities and staff and contractors can improve their personal skills and experience through relevant interactions with others outside the organisation.
- 1.5 This policy documents that every staff member has permission to use social media at work for work purposes. It sets out our expectations of you when you do so and what you can expect from us.
- 1.6 This policy is provided so that all staff; either directly employed or employed by the Trust on behalf of a third party organisation, are aware of their personal responsibilities for appropriate use of social media facilities they may access.
- 1.7 Trust employees are encouraged to maintain standards of professionalism and may be held to account for any inflammatory, derogatory, slanderous or abusive statements. Just as we don't tolerate bullying in real life, we will not tolerate it online.
- 1.8 Unless specifically authorised, it is important that staff members do not give the impression that their comments represent the views of the Trust, our staff or our hospitals.
- 1.9 The Trust has a responsibility to ensure the operational effectiveness of its business, including its public image, reputation and for the protection of its varied information assets. This involves ensuring confidentiality, appropriateness and maintaining security in accordance with the Trust's Information Governance policies, Human Resources Policies, UK legislation and best practice guidance.
- 1.10 This policy is issued and maintained by the Executive Director of HR / Director of NHIS on behalf of the Trust, at the issue defined on the front sheet, which supersedes and replaces all previous versions.

## **2 POLICY STATEMENT**

- 2.1 This policy is provided so that all staff; either directly employed or employed by the Trust on behalf of a third party organisation, are aware of their personal responsibilities for appropriate use of social media facilities they may access.
- 2.2 The Trust is committed to preventing discrimination, valuing diversity and achieving quality of opportunity. No employee will receive less favourable treatment on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation or on the grounds of trade union membership.
- 2.3 Please see the list of some of the policies below that are also relevant to this policy and should be read in conjunction with this policy:
- Confidentiality Policy
  - Whistleblowers Policy
  - Acceptable Use of the Internet and Email Policy
  - Disciplinary Procedures
  - Information Governance Policy
  - Information Governance Management Framework
  - Information Security Policy
  - Electronic Remote Working Policy

### **3 DEFINITIONS**

- 3.1 Definitions for specific terms used in the policy are clarified below:

‘The Trust’:	means the Sherwood Forest Hospitals NHS Foundation Trust
‘Staff ‘:	means all employees of the trust including those managed by a third party organisation on behalf of the Trust
‘NHIS’:	Nottinghamshire Health Informatics Service
‘Social Networking’:	the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. It involves building communities or networks, encouraging participation and engagement. Social networking is also known as “social software”, “social computing” and includes (but not exclusively) the definitions listed below. The use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook, Twitter and LinkedIn.
‘Social Media’:	the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others who often share the same community interests. Such technologies can include blackberry messaging, instant messaging and other similar services etc.

‘Social Engineering’: the method whereby an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation’s staff or maintenance contractor etc.

‘Blagging’: the term commonly used to describe the deliberate, reckless and potentially criminal obtaining and/or disclosing of personal information about individuals without that person’s knowledge or valid consent. Recent media reports allege that blagging is an issue that may particularly affect individuals who are of media interest but may potentially affect anyone.

The terms Social Engineering and Blagging are sometimes used interchangeably to describe methods of hacking into systems including phone services or where trickery is used to fool people into disclosing confidential information. Guidance is provided below in order to help clarify these issues for NHS organisations and their staff.

‘Blogging or Tweeting (micro-blogging)’:

using a public website to write an online diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video. Many blogs and tweets are interactive allowing visitors to respond leaving comments or to potentially send messages to others. It is increasingly common for blogs to feature advertisements to financially benefit the blogger or to promote a blogger’s favourite cause. The word blog is derived from the phrase weB LOG. Examples of these websites include Twitter.com and Blogging.com

## **4 ROLE AND RESPONSIBILITIES**

- 4.1 All members of staff will read and note the contents of this policy and must have access to and must follow the guidance outlined in the Trust’s policies and procedures.
- 4.2 All staff are responsible for ensuring that no actual or potential information breaches occur as a direct result of their actions.
- 4.3 The Trust will investigate all suspected/actual information breaches and report through their incident reporting procedures.
- 4.4 Staff who become aware of an actual or potential information breach or communications that have the potential to damage the reputation of the Trust, has a responsibility to report it to their line manager and/or HR

## **5 SCOPE OF POLICY**

- 5.1 The policy applies to all employees employed on Agenda for Change terms and conditions of service, to temporary workers/contractors/agency workers, students on placement, volunteers, and staff covered by Medical & Dental conditions of service.

## **6 CONSULTATION**

- 6.1 The consultation process for this policy is as follows:

- Local Health Community Information Governance Forum
- NHIS Compliance, Risk, Assurance Management group
- Organisation led Information Governance Groups and internal Board structures.
- Joint staff partnership forum

## **7 DUTIES AND RESPONSIBILITIES - Private Use of Social Media**

- 7.2 Staff should be aware that the Trust reserves the right to use legitimate means to scan the web, including social networking sites for content that it finds inappropriate. The Trust also reserves the right to monitor staff business usage of social networking sites during work time.
- 7.3 Staff are encouraged not to divulge who their employers are within their personal profile pages (e.g. in accordance with the Royal College of Nursing (RCN) guidelines "RCN Legal Advice on using the internet"). However, those that do divulge their employer should state that they are tweeting/blogging etc. in a personal capacity.
- 7.4 Staff are ultimately responsible for their own online behaviour both during and outside of designated working hours. Staff must take care to avoid online content or actions that are inaccurate, libellous, defamatory, discriminatory, harassing, threatening or may otherwise be illegal. Staff should be aware that failure to adhere to this policy may be viewed as Gross Misconduct and action will be taken in line with Trust Disciplinary Procedures, which may lead to dismissal. It is also possible for staff to be subject to civil proceedings or criminal prosecution.
- 7.5 Staff are not authorised to communicate by any means on behalf of the Trust unless this is an accepted normal part of their job, or through special arrangement that has been approved in writing in advance by the Head of the Communications Team. No social media sites or pages relating to the Trust should be set up by staff without prior approval from the Communications Team. See appendix B/C
- 7.6 Staff who use Social Media must not disclose information of the Trust that is of a sensitive or confidential nature e.g. person identifiable information regarding other staff or patients, or that is subject to a non-disclosure contract or agreement. This applies to information about service users, other staff and contractors, other organisations, commercial suppliers and other information about the Trust and its business activities.
- 7.7 Corporate logos or other visible markings or identifications associated with the Trust may only be used for official business related to the Trust where prior written permission has been obtained from the Head of the Communications Team.

- 7.8 Staff must not share details of the Trusts implemented security or risk management arrangements. These details are confidential, may be misused and if circumvented could lead to a serious breach of security occurring.
- 7.9 Staff who may not directly identify themselves as Trust staff members when using social networking sites for personal purpose at home should be aware that the content they post on Social Media sites could still be construed as relevant to their employment with the Trust.
- 7.10 Unauthorised disclosure of confidential information would constitute Gross Misconduct and will be dealt with in accordance with the Trusts Disciplinary Procedure which may lead to dismissal.
- 7.11 When using social networking sites, staff should respect their audience. Staff should not make any detrimental comments about colleagues whilst using Social Media sites, e.g. failing to show dignity at work (harassment), discriminatory language, personal insults and obscenity. These examples are not exhaustive and will be considered a disciplinary matter in line with the Trust Disciplinary policy and procedure which may lead to dismissal.
- 7.12 The Trust may also take disciplinary action, if necessary, against any staff member who brings the organisation into disrepute by inappropriate disclosure e.g. comments and photographs on social networking sites or personal internet sites.

## **8. DUTIES AND RESPONSIBILITIES - Trust Use of Social Media**

- 8.1 The Trust has a corporate presence on Facebook, Twitter, LinkedIn, Vimeo and You Tube and if staff wish to convey news stories, events or messages through these channels, then this must be done with prior written authorisation from the Head of the Communication Team.

## **9. REPORTING INAPPROPRIATE BEHAVIOUR ON SOCIAL MEDIA**

- 9.1 If a member of staff witnesses information contained in Social Media sites that contravenes this policy, they should report the issue through the Trust Incident Reporting process and their line manager and/or HR.
- 9.2 All incidents will be investigated by the appropriate Division with support provided by the Information Governance Team and the Human Resources Department where necessary.

## **10 EVIDENCE BASE**

- 10.1 The legal obligations of the Trust and the NHS as a whole can be found in the NHS Information Governance Guidance on Legal and Professional Obligations (DH, 2007) which is available on the Internet and this policy must be read in the context of and with reference to these legislations and guidance.

## **11 MONITORING COMPLIANCE**

- 11.1 The Trust reserves the right to use legitimate means to scan the web, including

Social Media sites for content that it finds inappropriate.

- 11.2 The Trust reserves the right to monitor the usage of Social Media sites during working hours.
- 11.3 A review of this policy will be conducted every two years or following a change to associated legislation and/or national guidance or national/local terms and conditions of service.
- 11.4 The responsibility for this policy and staff guidance is delegated to the Executive Director of Human Resources.

## **12 TRAINING REQUIREMENTS**

- 12.1 It is the responsibility of the Trust to ensure that mandatory training and induction programmes are implemented to ensure the awareness of all staff with regard to Trust Policy and procedure.
- 12.2 It is the responsibility of all Line Managers to ensure that their staff attend mandatory Information Governance training on an annual basis, and pro-actively encourage compliance with this policy.

## **13 DISTRIBUTION**

- 13.1 The policy, once approved, will be included within the Corporate Information section of the Trust's Intranet.

## **14 COMMUNICATION**

- 14.1 On approval the policy will be communicated to all existing staff via Team Brief, the weekly staff bulletin and the 'Latest Updates' section of the Trust's Intranet homepage for implementation purposes.
- 14.2 New members of staff will be informed of the policy at Induction and by their Line Managers.

## **15 AUTHOR AND REVIEW DETAILS**

Date issued:	January 2016
Date to be reviewed by:	January 2018
To be reviewed by:	Information Governance Manager / HR / Communications
Executive Sponsor:	Executive Director of HR / Director of NHIS

## **16 APPENDICES**

Appendix A – Potential Risks to the Trust of Staff Using Blogging and Social Networking

## **APPENDIX A: POTENTIAL RISKS TO THE TRUST OF STAFF USING BLOGGING AND SOCIAL NETWORKING**

A range of potential risks and impact consequences exist that staff should be aware of:

### **1. Unauthorised disclosure of business information and potential confidentiality breach**

Blogging and social networking sites can provide an easy means for sensitive or confidential information to leak from an organisation, either maliciously or otherwise. Once loaded to a blogging or social networking site, Trust information enters the public domain and may be processed, stored and reused anywhere globally. In short, Trust control can be lost and reputational damage can easily occur.

### **2. Malicious attack associated with identity theft**

Most blogging and social networking sites allow users to create a personal profile. People often place a large amount of personal information on social networking sites, including photographs, details about their nationality, ethnic origin, religion, addresses and date of birth, telephone contact numbers, and interests. This information may be of use to criminals and others who are seeking to steal or reuse identities or who may use the information for social engineering purposes.

### **3. Legal liabilities from defamatory postings etc. by staff**

When a person registers with a website they typically have to indicate their acceptance of the sites terms and conditions. These can be several pages long and contain difficult to read and understand legal jargon. Such terms and conditions may potentially give the site 'ownership' and 'third party disclosure' rights over content placed on the site, and could create possible liabilities for the Trust that allows employees to use them. For example, where a staff member is registering on a website from a computer/electronic device within the Trust, it may potentially be assumed that the user is acting on behalf of the Trust and any libellous, inflammatory or derogatory comments may result in civil litigation or criminal prosecution. In addition, information being hosted by the website may be subject to other legal jurisdiction overseas and may be very difficult to correct or remove.

#### **3.1 Reputational damage**

Ill-considered or unjustified comments left on sites may adversely affect public and professional opinion toward an individual, their employer or another implicated organisation, contractor, service provider or business partner etc. This can lead to a change in social or business status with a danger of adverse consequential impacts and possibility of legal proceedings.

#### **3.2 Malicious code targeting social networking users causing virus infections and consequential damage to end user devices**

Blogging and social networking sites may encourage or require the download and installation of additional code in order to maximise the sites functionality and potential values. Where

such sites have weak or ineffective security controls it may be possible for its operating system or application code to be changed to contain malicious content such as Viruses and Trojans, or to trigger unintended actions such as Phishing – a way of obtaining sensitive information through bogus impersonation as a trustworthy entity.

### **3.3 Systems overload from heavy use of sites with implications of degraded services and non-productive activities**

Blogging and social networking sites can pose threats to an organisation's own information infrastructure. Particularly as the use of rich media (such as video and audio) becomes the norm in such sites, the network bandwidth consumption generated by these sites can be significant and they have the potential to be the biggest bandwidth consumers within an organisation. In an aggregated sense widespread use of blogging and social networking sites may introduce new capacity issues for local and national NHS infrastructure and services.

### **3.4 Staff intimidation or harassment with the possibility of personal threat or attack against the blogger, sometimes without apparent reason**

Other online bloggers can hold strong views and may potentially be offended at what they read, however unlikely or unintended that might seem. In extreme cases this negative reaction could lead to targeted attack or assault against the original blogger with potential to cause them anxiety, distress and personal safety issues.

## **APPENDIX B– STAFF GUIDANCE ON THE USE OF SOCIAL MEDIA SITES**

This guidance should be read in conjunction with the Trust's Acceptable Use of the Internet & Email Policy.

### **HOW TO AVOID PROBLEMS WITH BLOGGING AND SOCIAL NETWORKING SITES**

1. When registering with a website, understand what you are signing up to by reading the terms and conditions carefully and importantly determine what security, confidentiality and liability claims, undertakings and exclusions exist. If in any doubt seek the advice from the Information Governance and/or Communications Team.
2. Be careful about the personal details you post online such as contact details, date of birth, your profession, your organisation. Such information could put you at risk of identity fraud.
3. Think about what you want to use your online profile for, applying appropriate security and preferences settings as necessary.
4. Keep your password safe and avoid obvious ones that others might easily guess.
5. Be aware of your personal responsibility for the words you post and also for the comments of others you allow on your blog or webpage.
6. Do not post anything online that may cause offence or distress to other users or is likely to damage the reputation of yourself or the Trust.
7. Avoid unattributable anonymous comments.

8. Be suspicious of all unsolicited contacts. This can include phone calls, visits, faxed messages, email, SMS (Short Message Service) messages etc. from anyone asking about information about other staff, contractors, patients, service users or other potentially confidential information.
9. Where a new contact claims to be a legitimate member of staff or a business partner organisation, ensure you take steps to verify their identity and business needs directly with their department head or other organisation.
10. Do not provide information about your organisation, its service users or other individuals including structures and networks unless you are certain of the recipient's identity and their authority to have access to that information. Check that the intended recipient has appropriate information governance arrangements in place to handle any information disclosed to them.
11. Avoid disclosing personal or sensitive information by email. Where this is necessary ensure the recipient's email address is verified and legitimate, and that appropriate data encryption standards are used for patient/client and other sensitive information. If in doubt please contact the NHIS Service Desk for further advice.
12. Do not send personal or other sensitive information over the Internet unless this has been approved by your Line Manager and the Information Governance department.
13. In the event that you think you may have been a social engineering or blagging victim ensure you immediately report this as an incident in accordance with the Trust Incident Reporting Policy. Additional advice can be provided by the Information Governance Team and/or Human Resources department where necessary. It is possible that a notice may be issued to other staff within the Trust with appropriate guidance to be alert to any new, unusual or suspicious activity.

#### **APPENDIX C - COMMUNICATIONS THAT EMPLOYEES MAKE IN A PERSONAL CAPACITY THROUGH SOCIAL MEDIA MUST NOT:**

- Bring the Trust into disrepute by criticising or arguing with customers, colleagues or rivals; making defamatory comments about individuals or links to inappropriate or inappropriate content.
- Breach confidentiality for example by revealing information owned by the organisation; giving away confidential information about an individual (such as a colleague or customer contact); discussing the Trust's internal workings or its future business plans that have not been communicated to the public.
- Breach copyright for example by; using someone else's images or written content without permission; or failing to give acknowledgement where permission has been given to reproduce something.
- Do anything that could be considered discriminatory against, or bullying or harassment of any individual, for example by, making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality, disability, sexual orientation, religion or belief or age;
- Using social media to bully another individual or posting images that are

discriminatory or offensive (or links to such content). Incidents of discrimination, bullying or harassment which take place via social media will be managed in line with the Trust Disciplinary Policy.

- Only the Communications Team can conduct campaigns on social media, as it has responsibility for external communications.
- Written permission should be requested from the Communication Team before developing a Trust project presence in any form of social media. The request must describe which social media is involved, the nature of the Trust project presence, the purpose of the presence, a risk analysis, how the presence is to be resourced and managed, how the information on the social media site will be stored for FOI purposes and finally an exit strategy.
- A copy of the business case must be submitted at the same time to the Communications Team for comment.
- You must respect copyright, fair use and financial disclosure rules.

## **SOCIAL MEDIA DOS AND DON'TS**

Sherwood Forest Hospitals recognises the value social media platforms such as Facebook, LinkedIn and Twitter can bring to its employees. We are aware many staff use social media networks in their own time, using their own computers and smartphones.

Every staff member has permission to use social media at work for work purposes. Social media offers some great ways to really grow your professional network, discover new ideas, share learning and best practice, and take your career to the next level.

However, it is the responsibility of everyone within the Trust to use social media responsibly. Although members of staff are not acting on behalf of the organisation when using social media they must be mindful that their online posts could potentially be damaging to the Trust if they are inaccurate or flippant.

Please remember that when you use these sites, as Trust employees, you are encouraged to maintain standards of professionalism and may be held to account for any inflammatory, derogatory, slanderous or abusive statements. Just as we don't tolerate bullying in real life, we will not tolerate it online. Such activity can amount to misconduct and employers will need to take disciplinary action for inappropriate behaviour exposed by social media or inappropriate comments made on social media.

Please consider what you do, who you work for and who this affects before you post anything online. Sign up to the updated social media policy on the intranet and check these handy dos and don'ts.

### **DO:**

- Use social media responsibly

- Share good practice. Have you or your team done something great then let people know.
- Celebrate success
- Keep your comments light and positive. If you can't, don't comment.
- Read the Trust social media policy
- Be open about who you are and be clear that your views are your own, and not those of the Trust
- Respect copyright laws and credit the work of others
- Think "does this reflect badly on the Trust, the hospitals or our staff?" - if it could, don't post!

#### **DON'T:**

- Post anything that could damage the Trust, its brand or its reputation
- Post photographs of patients, their families and carers, visitors or staff within the hospital grounds
- Try to hide your identity
- Abuse or attack the Trust, the hospitals, our partners, staff or patients
- Post any confidential, sensitive or otherwise misleading information
- Set up any Trust group without the express permission of the communications team

If in doubt, ask a member of the communications team or email [e.communications@sfh-tr.nhs.uk](mailto:e.communications@sfh-tr.nhs.uk)