

The Newcastle upon Tyne Hospitals NHS Foundation Trust

Employment Policies and Procedures

Use of Social Media Policy

Version No.:	1.2
Effective From:	12 September 2013
Expiry Date:	12 September 2016
Date Ratified:	7 August 2013
Ratified By:	Employment Policies & Procedures Consultative Group

1 Introduction

- 1.1 This policy relates to the use of social media activities conducted on-line outside of work and the posting of material, images, comments, blogs or tweets on such sites.
- 1.2 Social media refers to a broad range of websites and services that allow people to connect with others on-line. Social networking and blogging websites (such as *Facebook, Bebo, Twitter, MySpace and Blogging.com*) are perhaps the most well known examples of social media, but the terms of this policy cover all web-based services.
- 1.3 The Trust acknowledges that social media provides a number of benefits in which staff may wish to participate in their personal life. However, staff are expected to use sites appropriately, and in ways that are consistent with:
- the Trust's values and policies,
 - their individual responsibilities as an employee, and
 - relevant codes of professional conduct (where applicable)
- 1.4 The use of social media by staff (both at work or in their personal life) can potentially expose the Trust to information risks. The Trust may be liable for acts of bullying and harassment by staff even where the harassment takes place outside of the workplace. All staff must follow the guidelines below in relation to any social media they use or access. Staff are personally responsible for any information they place onto social media web sites.

2 Scope

The policy applies to all employees including, honorary contract holders, researchers, trainees, clinical attachments/observers, agency staff, Bank workers, volunteers, contractors and other individuals involved in patient care.

3 Aims

- 3.1 The purpose of this policy is to outline the responsibilities of staff in relation to their use of social networking websites, and highlight areas where potential problems can arise for staff and/or the Trust.

4 Duties (Roles and responsibilities)

- 4.1 The Executive Team is accountable to the Trust Board for ensuring Trust-wide compliance with policy.
- 4.2 Directorate managers and heads of service are responsible to the Executive Team for ensuring policy implementation.
- 4.3 Managers are responsible for ensuring policy implementation and compliance in their area(s).
- 4.4 Staff are responsible for complying with policy.

5 Definitions

- 5.1 Social Media is the term commonly used for web-based and other mobile communication technologies that enable messages and opinions to be shared in dialogue with others.
- 5.2 Social Networking is the use of interactive web-based sites that mimic some of the interactions that occur between people. The sites enable people to exchange information about themselves, share pictures and videos and use blogs, tweets and private messaging to communicate with friends and others.
- 5.3 Blogging or tweeting is the use of a public website to write an on-line diary (known as a blog) sharing thoughts and opinions on various subjects. Many blogs or tweets are interactive allowing visitors to send messages to others.
- 5.2 Defamation is the act of making an unjustified statement about a person or organisation that is considered to harm their reputation.
- 5.3 Cyber-bullying occurs where the perpetrator's use of information technology creates an intimidating, hostile, degrading, humiliating or offensive environment for the victim.

6 General Principles

- 6.1 At no time should social media sites be accessed from Trust equipment (whether at work or outside of work). All social media sites are subject to automated blocking as part of the Trust's Internet Security Policy. Access to social media

sites at work have been designated inappropriate. The Trust acknowledges that staff may use their own hand held devices to access social media websites while at work, but usage must not be in work time.

- 6.2 The Trust respects all staff have rights to a private life, but this does not preclude the Trust taking into account actions outside of work. The Trust must ensure that confidentiality and its reputation are protected. Staff are expected to behave appropriately at all times and avoid on-line content or actions that are inaccurate, libellous, defamatory, harassing, threatening, discriminatory or may otherwise breach Trust policy or legislation. Staff are reminded that they are ultimately responsible for their own on-line behaviour. It is possible for staff to be subject to civil proceedings or criminal prosecution.
- 6.3 When a user registers with a site they typically have to indicate their acceptance of the site's terms and conditions. Such terms and conditions may give the 'site ownership' and 'third party disclosure' rights over content placed on the site and could create possible liabilities for the Trust such as action around defamation which could be lodged both against the individual and the organisation.
- 6.4 Risks associated with the use of social media include:
- unauthorised disclosure of Trust information and breaches of confidentiality
 - legal liabilities from defamatory postings
 - reputational damage
 - identity theft

7 Protecting the Trust and the individual

- 7.1 Through inappropriate use of social media websites staff may damage the Trust's or the individual's reputation or the reputation of related third parties, whether deliberately or unintentionally, and breach Trust policies including, but not restricted to:
- Email and Electronic Communications Policy
 - Internet Security Policy
 - Dignity and Respect at Work Policy
 - Disciplinary Policy and Procedure
 - Employee Wellbeing Policy (Incorporating Absence Management Procedure)
 - Confidentiality and Security (Data Accreditation)
- 7.2 Social media sites can increase the likelihood of inappropriate boundary transgressions, particularly where only a professional relationship previously existed. Difficult ethical issues can arise if, for example, clinical staff become party to information about patients that has not been disclosed as part of a clinical consultation.

- 7.3 Many professional codes of practice are explicit that registrants must uphold the reputation of the profession and inappropriate behaviour may be considered as misconduct by the profession.
- 7.4 The ethical and legal duty to protect patient confidentiality applies equally on the internet as to other media. Although individual pieces of information may not alone breach patient confidentiality, the sum of published information across a number of online platforms could be sufficient to identify individuals.
- 7.5 Staff using social media websites must:
- refrain from identifying themselves as working for the Trust, this includes ensuring any on-line profile does not refer to the Trust or could be linked to the Trust. Staff must be mindful that although they may not explicitly reveal themselves as Trust staff, their comments, videos, photographs or postings could identify a link with the Trust. Staff must not use Trust images, logos or any forms of Trust communications/documents without express permission.
 - refrain from disclosing or using a Trust email account
 - ensure the Trust is not brought into disrepute e.g. by criticising or posting inappropriate comments about the Trust, colleagues, patients or related third parties; by posting images that are inappropriate or linked to inappropriate content; or by pursuing personal relationships with patients or service users
 - ensure confidentiality is maintained by not revealing sensitive or confidential information about colleagues, patients, visitors or the Trust, including, but not restricted to Trust policy and plans or details of internal discussions
 - ensure there are no breaches of copyright by using images or written content without permission
 - not distribute sexually explicit material
 - not bully or intimidate colleagues, patients or individuals connected with your work within the Trust.
 - not do anything that could be considered discriminatory against or towards any individual by making offensive or derogatory comments relating to gender, gender reassignment, race (including nationality), disability, sexual orientation, age, religion or belief, marriage and civil partnership or pregnancy and maternity
 - use the same safeguards they would with any form of communication about the Trust in a public sphere
 -

- not use social media sites in any way which is unlawful
- not knowingly enter into relationships with patients, their relatives or carers on social media sites
- remove offending content immediately if asked to do so
- ensure that if your social media account is hacked, the incident is reported to the sites administration and a record is maintained of any bogus information posted on the account. If the incident or the nature of the material is in danger of breaching Trust policy, staff must notify their line manager immediately.

7.6 All fraudulent/inappropriate activity in breach of this or any of the Trust's policies and procedures will be subject to investigation in accordance with the Disciplinary Policy and Procedure. This may result in formal action. The Trust reserves the right to use legitimate means to scan the web for content and will follow up on information about staff which is brought to its attention.

7.7 Serious breaches of this policy (e.g. incidents of bullying, harassment or social media activity causing serious damage to the Trust's reputation) may constitute gross misconduct and may lead to summary dismissal.

7.8 Patients or visitors who utilise social media to be abusive or defamatory in relation to Trust staff or who harass staff via social media, will be deemed to be engaging in inappropriate behaviour and actions will be undertaken in line with the Trust Policy for the Exclusion from Treatment of Violent or Abusive Patients.

8 Respecting others when using Social Media

8.1 Social media allow photographs, videos and comments to be shared, however, it is not appropriate to share work-related information in this way. Images taken at work or work related Trust events should not appear publicly on staff members' social media accounts.

8.2 Staff must be considerate of all colleagues and not post pictures without permission. If requested, staff must remove information about a colleague if that colleague asks them to do so.

8.3 Under no circumstances should offensive or inappropriate comments be made about colleagues, patients or visitors on the internet. This may amount to cyber bullying and will be subject to action in accordance with the Disciplinary Policy and Procedure.

8.4 Some types of bullying and harassment may constitute unlawful discrimination. Allegations may give rise to the possibility of civil claims or criminal proceedings against the offending member of staff. Such action would proceed independent

of any internal disciplinary proceedings. The alleged harasser could be personally liable to pay compensation to the complainant if a successful complaint in an Employment Tribunal or other Court was brought against them. Criminal proceedings could lead to conviction and criminal penalties.

- 8.5 Defamation can apply to any comments posted on the web, irrespective of whether they are made in a personal or professional capacity. If an individual makes a statement that is alleged to be defamatory, it could result in legal action against the individual and the Trust.

9 Security and Identity Theft

- 9.1 Staff should be security conscious and should take steps to protect themselves from identity theft by restricting the amount of personal information made available.
- 9.2 Staff should be aware that social media are public forums, particularly if part of a network, and should not assume their entries on any form of social media will remain private. Potentially, anything said, shown or received could be made available to an audience wider than that originally intended.
- 9.3 Many social media sites have privacy settings that allow users to control and place restrictions on who has access to their personal information. The default settings on such sites often permit various types of content to be shared beyond an individual's network of friends. It is important that staff familiarise themselves with the privacy provisions for different social media applications. It is recommended that staff consider adopting conservative privacy settings where they are available and ensure they apply at all times.
- 9.4 It should be noted that not all content on the web can be protected in this way and some social media applications do not provide flexible privacy settings.

10 Whistleblowing

All staff should be aware that the Public Interest Disclosure Act 1998 gives legal protection to employees who wish to "whistleblow" any concerns. The Act makes it clear that the process of "whistleblowing" or "speaking up" normally involves raising the issue internally first. The Trust's Whistleblowing Policy (A Policy on Voicing Concerns about Suspected Wrong-doing in the Workplace) sets out the various means of raising concerns. Using social media to whistleblow without already having raised concerns through the proper channels would not normally be considered appropriate.

11 Reporting of adverse incidents

- 11.1 Alleged breaches of this policy should be reported to the IT Service Desk who will record the following:
- name and contact details of the person reporting the matter
 - location of the website and content which is considered inappropriate
 - how/why the content is considered inappropriate
- 11.2 The IT Service Desk will inform the relevant line manager and the Senior Human Resources Manager. If the incident involves patient identifiable information, the Caldicott Guardian will also be informed.
- 11.3 The Trust reserves the right to secure the removal of any such statement/ content and will handle an alleged breach in accordance with the Disciplinary Policy and Procedure.
- 11.4 Staff are required to cooperate in investigations and provide password and log-in details where necessary.
- 11.5 If staff believe they have been subject to cyber bullying by another member of staff or someone connected to the Trust, they should report the behaviour immediately to their line manager.
- 11.6 If a member of staff feels they have inadvertently breached the Trust's Use of Social Media Policy they must attempt to rectify the breach immediately and must advise their line manager without delay.

12 Training

Training will be provided by the Human Resources Department to managers following implementation of the procedure.

13 Equality and diversity

The Trust is committed to ensuring that, as far as is reasonably practicable, the way services are provided and the way staff are treated reflects their individual needs and does not unlawfully discriminate against individuals or groups. This policy has been properly assessed.

14 Monitoring compliance with the policy

Standard / Process / Issue	Monitoring and Audit			
	Method	By	Committee	Frequency
The number of disciplinary cases relating	Reporting of information held	Director of Human	Heads of Human	Annually

to the use of Social Media will be audited	in ESR	Resources	Resources Meeting	
--	--------	-----------	-------------------	--

15 Consultation and review of this policy

This policy has been reviewed in consultation with the Employment Policies and Procedures Consultative Group

16 Implementation of the policy (including raising awareness)

A summary of the key changes will be notified to managers following implementation. Further advice and guidance will be available from the Human Resources Department.

17 References

- 1) Equality Act 2010 available at <http://www.legislation.gov.uk/ukpga/2010/15/contents>
- 2) Public Interest Disclosure Act 1998 available at <http://www.legislation.gov.uk/ukpga/1998/23/contents>

18 Additional documents

- [Confidentiality and Security \(Data Accreditation\)](#)
- [Dignity and Respect at Work Policy](#)
- [Disciplinary Policy and Procedure](#)
- [Email and Electronic Communications Policy](#)
- [Employee Wellbeing Policy \(Incorporating Absence Management Procedure\)](#)
- [Exclusion from Treatment of Violent or Abusive Patients](#)
- [Internet Security Policy](#)
- [Maintaining Professional Boundaries Policy](#)
- [Whistleblowing Policy](#)

Author: Employment Policies and Procedures Consultative Group

THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST
IMPACT ASSESSMENT – SCREENING FORM A

This form must be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

Policy Title:	Use of Social Media Policy	Policy Author:	Mrs W Johnson – HR Manager (Projects)
		Yes/No?	You must provide evidence to support your response:
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of the following: (* denotes protected characteristics under the Equality Act 2010)		Policy applies does not affect any group more or less favourably than another and is underpinned by the Trust’s overriding policy on Equal Opportunities.
	• Race *)
	• Ethnic origins (including gypsies and travellers))
	• Nationality)
	• Gender *) see above
	• Culture)
	• Religion or belief *)
	• Sexual orientation including lesbian, gay and bisexual people *)
	• Age *)
	• Disability – learning difficulties, physical disability, sensory impairment and mental health problems *)
	• Gender reassignment *)
	• Marriage and civil partnership *)
2.	Is there any evidence that some groups are affected differently?		There is no evidence to support any group is affected differently
3.	If you have identified potential discrimination which can include associative discrimination i.e. direct discrimination against someone because they associate with another person who possesses a protected characteristic, are any exceptions valid, legal and/or justifiable?		n/a
4(a).	Is the impact of the policy/guidance likely to be negative? <i>(If “yes”, please answer sections 4(b) to 4(d)).</i>		No
4(b).	If so can the impact be avoided?		n/a
4(c).	What alternatives are there to achieving the policy/guidance without the impact?		n/a
4(d).	Can we reduce the impact by taking different action?		n/a

Comments:	Action Plan due (or Not Applicable):
------------------	---

Name and Designation of Person responsible for completion of this form: Mrs W Johnson, HR Manager (Projects) Date:.....10 April 2013

Names & Designations of those involved in the impact assessment screening process: Employment Polices and Procedures Consultation Group.....

_(If any reader of this procedural document identifies a potential discriminatory impact that has not been identified on this form, please refer to the Policy Author identified above, together with any suggestions for the actions required to avoid/reduce this impact.)