



## Use of Digital Media (including Social Media and/or Networking Sites) Policy

Document Status	Final
Version:	2.0

DOCUMENT CHANGE HISTORY		
Initiated by	Date	Author
Ann Langdon	June 2012	Sarah Atkins
Version	Date	Comments (i.e. viewed, or reviewed, amended approved by person or committee)
Draft v0.1	June 2012	Initial draft by Sarah Atkins
Draft v0.2	July 2012	Review by HR Policy Group
Draft v0.3	17 October 2012	Circulated for comment to Marcus Bailey, Sarah Atkins and Paul Sexby (CEOP);
Draft v0.4	19 October 2012	Reviewed by HR Policy Group
Draft v0.5	22 October 2012	Reformatted by Sarah Atkins
Draft v0.6	9 November 2012	Incorporated comments from Chris Hartley and Marcus Bailey
Draft v0.7	16 November 2012	Review and comments by Tracey Leghorn. Forwarded to Sarah Atkins.
Draft v0.8	23 November 2012	Reviewed by HR Policy Group
Draft v 0.9	24 January 2013	Comments by Communications Dept for review by HR Policy Group
Draft v 0.10	28 January 2013	Amendments made by HR Policy Group
Draft v 0.11	1 March 2013	Recommended by Staff Partnership Forum
V1.0	March 2013	ELT Approved
V2.0	10 December 2015	Approved extension to review date by SPF to March 2016

Document Reference	HR Directorate
Recommended at Date	Staff Partnership Forum 1 March 2013

Approved at Date	Executive Management Team
Review date of approved document	March 2016
Equality Impact Assessment	13 November 2012
Linked procedural documents	Dignity at Work Policy Disciplinary Policy (Managing Conduct and Performance) Digital Communications Strategy Internet Use Policy Personal Use By Staff of Social Media Policy Use of Photography CSOP 2.3
Dissemination requirements	All managers and staff, via staff bulletins and the intranet
Checklist completed?	Yes
Part of Trust's publication scheme	Yes/No

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), seconded staff and homeworkers.

All Trust policies can be provided in alternative formats.

## Contents

Paragraph	Title
<b>1</b>	<b>Introduction</b>
<b>2</b>	<b>Purpose</b>
<b>3</b>	<b>Duties</b>
3.1	Human Resources Department

3.2 Managers, HR and Trade Union Representatives

3.3 Employees

3.4 Consultation and communication with stakeholders

## **4 Definitions**

## **5 Development**

5.1 Prioritisation of work

5.2 Identification of stakeholders

5.3 Responsibility for Document's Development

## **6 The Scope of Social Networking**

6.1 Trust access

6.2 Third party access

## **7 Employee Conduct**

7.1 Everyday use

7.2 Expected standards

7.3 Disclosing employment

7.4 Contact from a third party

7.5 Wellbeing

7.6 Potential outcomes

## **8 Personal Profiles/Blogging**

8.1 Attributing profiles to the Trust

8.2	Managing your profile
<b>9</b>	<b>Imagery</b>
9.1	Sharing/posting of imagery
9.2	Production of photos
<b>10</b>	<b>Respecting others when using Social Networking sites</b>
<b>11</b>	<b>Accessing Social Network Sites Using the Trust's IT System</b>
11.1	Accessing social networks for the purposes of Trust business
<b>12</b>	<b>Identifying Individuals</b>
<b>13</b>	<b>Policy Review</b>
<b>14</b>	<b>Equality Impact Assessment</b>
<b>15</b>	<b>Dissemination and Implementation</b>
15.1	Dissemination
15.2	Implementation
<b>16</b>	<b>Process for Monitoring Compliance and Effectiveness</b>
<b>17</b>	<b>Standards/Key Performance Indicators</b>
<b>18</b>	<b>References</b>
<b>19</b>	<b>Associated Documents</b>

## **Paragraph**

Appendix A	Checklist for the Development or Review and Approval of Procedural Document
Appendix B	Monitoring Table
Appendix C	Impact Equality Assessment

## **1. Introduction**

This document outlines the Use of Digital Media Policy for The East of England Ambulance Service NHS Trust (the Trust). For the purpose of this policy any reference to digital media includes social media and/or networking sites. (examples of digital media are shown in section 6 of this policy).

The Trust's Internet Use Policy deals with the use of web-related systems whilst at work. This Policy sets out the principles which Trust staff are expected to follow when using digital media in their personal lives. The Internet involves fast moving technologies and it is impossible to cover all circumstances. However, the principles set out in this document should always be followed.

The intention of this Policy is not to stop Trust staff from conducting legitimate activities on the Internet, nor to stifle constructive criticism, but serves to highlight those areas in which problems can arise for both individual staff members and the Trust.

## **2. Purpose**

This policy aims to ensure that employee use of social media does not damage the Trust's reputation and that it maintains patient confidentiality and an environment where individuals are treated with dignity and respect.

This policy encompasses employee's personal use of social networking and also their use of online services as part of the Trust's communication strategy

## **3. Duties**

### **3.1 Human Resources Department**

The Human Resources Department is responsible for keeping the provisions within this policy in line with employment legislation, best practice people management principles and NHS guidelines.

### **3.2 Managers, HR and Trade Union Representatives**

Managers, HR staff and trade union representatives are responsible for providing advice and guidance to employees on the application of this policy and procedure.

### **3.3 Employees**

Employees are responsible for making every effort to provide information and documentation that is requested of them or they feel relevant to the operation of this policy and also for complying with the processes and agreements contained within this policy.

### **3.4 Consultation and Communications with Stakeholders**

It is approved by the Staff Partnership Forum, which includes representatives from Unison, HR and Management. This policy has been written in partnership by management and staff side, and in accordance with current employment legislation.

Once published any individuals can submit comments and/or suggestions to the HR Policy Group via a dedicated email address ([hrpolicies@eastamb.nhs.uk](mailto:hrpolicies@eastamb.nhs.uk)) in relation to this Policy.

## **4. Definitions**

Digital Media – For the purpose of this policy this includes any internet based medium which enables users to communicate their thoughts, opinions or observations with the online community.

Trolling – Where a social networking user writes a deliberately provocative posting with the aim of inciting an angry response, usually with contents that are hurtful and/or personal.

## **5. Development**

### **5.1 Prioritisation of Work**

This policy has been developed to offer guidance to all managers about the expected level of conduct when using digital media sites.

### **5.2 Identification of Stakeholders**

Primary stakeholders are the Chief Executive, Director of Human Resources and Organisational Development, the Associate Director of Human Resources and the Human Resources (HR) Department. Also the Information Management & Technology Department and the Communications and Engagement Department.

### **5.3 Responsibility for Document's Development**

The HR Department are the authors of this Policy. It is recommended by the HR Policy Group to the Trust's Staff Partnership Forum and Executive Management Team for ratification.

## **6. The Scope of Digital Media**

The Trust defines digital media as any internet based medium which enables users to communicate their thoughts, opinions or observations with the online community. These sites include, but are not limited to:

- Facebook
- Twitter
- LinkedIn
- Google Plus
- MySpace
- Bebo
- Online message boards/forums/chat rooms
- YouTube
- Flickr
- Any form of blogging, including weblogs
- Audio/video podcasts
- Discussion boards, e.g. Yahoo and Google Groups
- Collaborative information sharing sites, e.g. Wikipedia
- Online multiplayer gaming platforms, e.g. World of Warcraft
- Open access online encyclopaedias or reference pages which invite users to

edit and define particular topics e.g. Wikipedia, Urban Dictionary

These media provide a number of benefits in which Trust staff may wish to participate in their personal life. However, when someone clearly identifies their association with the Trust and/or discusses their work, they are expected to behave appropriately, and in ways that are consistent with the Trust's values and policies, their individual responsibility as a Trust employee, and with the relevant professional codes of conduct which apply to their role, for example, those that apply to for healthcare professionals and/or NHS managers.

Digital media sites, like Facebook, provide a great way for people to keep in touch with friends and colleagues. However, through the open or semi-open nature of such sites, it is also possible for third parties to collate vast amounts of information.

In relation to privacy, there is a perception for example, that because Facebook users can limit access to their Facebook profile to 'friends', that the information therein is confidential to those persons. For example, all photographs uploaded onto Facebook become the property of Facebook. There have been reported cases of Facebook users finding their photographs used by advertisers without their prior knowledge.

All Trust staff should be mindful of the personal information they disclose on social networking sites, especially with regards to identify theft. Making information such as your date-of-birth, your place of work, and other personal information publicly available can be high risk in terms of identity theft.

## **6.1 Trust access**

The rise of digital media which includes social networking sites such as Facebook, and online comments responding to stories in the press means that employees can post a great deal of information which can be circulated and proliferated rapidly at the touch of a button and becomes instantly accessible to the public,. The Trust is therefore in a position to access a range of written information and/or photographs relating to employees' behaviour outside of the working environment that carries the potential to affect their reputation and dignity within work, as this information enters the public domain and the subject loses control of its ownership.

## **6.2 Third party access**

Digital media has changed the way in which many people communicate. Employees should be aware of how the information they share can be used and possibly exploited by other internet users. Examples could include;

- Journalists may try and gain information about the Trust or particular incidents by reviewing social networking entries;
- Patients may wish to contact clinicians following an incident and use social networking sites as a gateway.

## **7. Employee Conduct**

### **7.1 Everyday use**

The Trust recognises that employees have the right to make use of digital and social media in their everyday lives, each with their own benefits and advantages when used appropriately. These sites have increasingly become part of people's day to day activities. The Trust has established corporate Facebook and Twitter accounts as a modern method of communicating with the public, patients and stakeholder organisations. However, it is expected that employees should use these sites responsibly and with restraint due to them being in the public domain.

Not only can digital media help to share professional best practice, but it can also form useful networks and become part of someone's hobbies and interests. Employees should remember to verify any information for accuracy when using user-lead information sites and also if they participate in such sites, they must expressly state that the views and comments made are the personal ones and are not related to the Trust. When reading or posting any professional advice, employees should remember the demographic of the intended audience, as well as the skill level of the author(s).

## **7.2 Expected standards**

Employees must remember that they are bound by their own professional code/standards of conduct, performance and ethics (where applicable) and other Trust policies when making use of, for example, the media referred to in section 6. Employees have a duty to conduct themselves in a professional manner.

Employees:

- Must not reveal any information about patients;
- Must not reveal confidential or personal information about other employees without their express permission;
- Must not reveal any information about incidents;
- Must not discuss work related tasks which may reveal confidential information; Should adhere to the Terms of Use of the relevant social media/website, as well as copyright, defamation, discrimination, harassment and other applicable laws as may apply.
- Must not engage in activities online which may bring the Trust into disrepute or that can be interpreted as slurs, demeaning or inflammatory to individuals and/or the Trust;
- Must not engage in activities online about another NHS organisation, third party, regulatory or voluntary organisation or that can be interpreted as slurs, demeaning or inflammatory to individuals and/or the organisation;
- Must act in a transparent manner when altering online reference material, especially if this is done from a Trust PC as it could appear that the Trust is endorsing or reinforcing a definition e.g. editing of Wikipedia;
- Must not establish false or parody accounts as a means of attacking or abusing employees, colleagues, patients or anybody connected to the work of the Trust. Including fabricating content to post on YouTube or similar sites.
- Must not use the digital media in any way to attack or abuse employees, patients or anybody connected to the work of the Trust;
- Must not post derogatory or offensive comments on the internet about employees, volunteers, patients or anybody connected to the work of the Trust;
- Shall not engage in any form of trolling towards any employees, volunteers, patients or anybody connected to the work of the Trust;
- Must not upload any videos filmed at Trust locations without the express permission of the Trust.

## **7.3 Disclosing employment**

Employees wishing to make use of particular professional sites which require users to confirm their employer name, professional qualifications and experience (e.g. LinkedIn), the principles set out above are to be considered before making any entries. Ensure that professional and personal uses are not confused and that the most appropriate social media channel is selected.

## **7.4 Contact from a third party**

If an employee is contacted by a third party (e.g. journalists, press or broadcasting) about EEAST Use of Digital Media (including Social Networking Sites) Policy v2.0

comments or entries made through a social networking site(s) which relate to the Trust or Trust business they should contact their line manager before responding. The line manager may wish to consult the Communications Team or Human Resources Department for advice and/or guidance

## **7.5 Wellbeing**

Employees are strongly advised not to post any possible work related issues on any social media (referred to in section 6) when feeling either upset and/or angry about a circumstance that may have occurred. It is recognised that when doing so inappropriate comments may well be made. Although you may later regret the fact that you made such comments it should be noted that once information has been posted online it can be incredibly difficult to remove it and prevent others from seeing it. Even with strict privacy settings, employees should always remember that they cannot guarantee how the information may be quoted, copied or shared by persons who may or may not have been the intended recipients at a later date. Employees are reminded that their line manager and/or the Employee Assistance Programme are available to talk through such issues.

## **7.6 Potential outcomes**

Employees who are found to breach of this policy will be managed in line with the Trust's Disciplinary policy. All employees are reminded of the need to maintain both patient and colleague confidentiality when using the different types of social media as outlined in this policy.

## **8. Personal Profiles/Blogging**

### **8.1 Attributing profiles to the Trust**

Sites such as Facebook and Twitter are designed for users to create profiles and share their views and experiences. There are also websites which host blogs; a form of online diary. Employees must decide whether they wish to expressly mention their current employer when completing their biography. Employees are advised that even if they decide not to disclose their employer, it may still be possible for users to link comments/disclosures with the Trust.

### **8.2 Managing your profile**

Employees are responsible, liable and accountable for the entries they post to their online profile.

If a third party makes an entry against your profile which could breach the principles set out within Section 7 above, employees must take a screen shot of the entry, remove the entry and contact their line manager to make them aware. If applicable it is advisable to report the breach to the social networking provider for them to take appropriate action.

If an employee's account becomes compromised, i.e. hacked, then the employee has a responsibility to resolve the matter by immediately removing all entries which have not been made by themselves and taking steps to ensure the security of their account. Employees who fail to take immediate action once they are made aware of a security concern will not be able to use this as mitigation in any Trust investigation.

Employees are responsible for maintaining the security and integrity of any passwords and pass-codes to social media sites. No passwords or pass-codes used in conjunction with Trust activities are to be used to access social media sites.

## **9. Imagery**

## **9.1 Sharing/posting of imagery**

Employees may not post imagery which depicts any Trust identifiable uniform, vehicle, crest or other branded resource in a negative light and/or may bring the Trust into disrepute. Additionally, photos may not be posted which:

- Reveal confidential information about a patient;
- Depict the day to day activity of the Trust in any form without prior consent of an appropriate manager;
- Knowingly compromise any on-going investigation by the Trust or a third party;
- May bring the Trust into disrepute.

## **9.2 Production of photos**

No photos may be taken during work time for the purposes of social networking, unless they are for the benefit of the Trust and are to be used through official communication streams.

It is becoming increasingly popular for members of the public to record our services for posting on social networking. Employees may not reference or link their profiles to such entries. Any instances of being filmed by the public whilst carrying out Trust business should be reported to a line manager as soon as possible.

## **10. Respecting others when using Social Networking sites**

Social networking sites allow photographs, videos and comments to be shared with thousands of other users. However, it may not be appropriate to share work-related information in this way.

For example, there may be an expectation that photographs taken at a private Trust event will not appear publicly on the Internet, both from those present and perhaps those not at the event. Staff should be considerate to their colleagues in such circumstances and should not post information when they have been asked not to. They should also remove information about a colleague if that colleague asks them to do so.

Under no circumstance should offensive comments be made about Trust colleagues, Trust business or patients on the Internet. This may amount to cyber-bullying and could be deemed a disciplinary offence.

## **11. Accessing Social Network Sites Using the Trust's IT System**

The Trust's IT system will deny employee access to the majority of social networking sites. However, where a site is available employees must note that engaging in any kind of online activity, which is not work related, is strictly prohibited.

### **11.1 Accessing social networks for the purposes of Trust business**

It may be necessary for designated members of staff to engage in social networking during work hours due to the nature of their role e.g. Communications. In cases where an employee believes they require such access, they must obtain permission from their line manager before using social networking sites and only then use them for justifiable business activities. In addition, the Trust's Digital Communications Officer should be made aware of the account details as all Trust associated social networking accounts will be monitored by the Communications Team.

Employees who access social networks on a Trust device must ensure they logout particularly if you share machines or use devices in a public space. If you do not log off your account may be accessed by other unauthorised people even if you quit the browser or turn the machine off.

## **12. Identifying individuals**

Employees involved in any of the following activities must not attempt to gain information about individuals and/or organisations through social networking. This is in order to protect themselves and/or the Trust from any assertion that they have gained information about a third party which could compromise any Trust process;

- Recruitment - unless an applicant specifically directs the recruiter to a site or area for the purposes of making their application;
- Procurement - unless a tender process requires the Trust to review information held online in a legitimate manner.

## **13. Policy Review**

This policy will be reviewed on an annual basis or amended in the light of new employment legislation and/or relevant case law.

## **14. Equality Impact Assessment**

An Equality Impact Assessment has been undertaken and is contained at Appendix C.

## **15. Dissemination and Implementation**

### **15.1 Dissemination**

This Policy will be disseminated to staff via the Trust intranet. Significant revisions and updates to the Policy will also be promoted in the staff bulletin.

### **15.2 Implementation**

Awareness of the Policy and compliance with its requirements will be promoted via Human Resources training sessions.

The HR Department will monitor staff compliance with the requirements of the Policy as part of their on-going work, and take action to rectify any perceived weaknesses in compliance as necessary.

## **16. Process for Monitoring Compliance and Effectiveness**

Areas of concern relating to social networking within EEAST will be monitored for compliance by the HR Department – see Appendix B - who will escalate any areas of concern to the Staff Partnership Forum.

## **17. Standards/Key Performance Indicators**

This work stream has been led from a continued increase in employees engagement with social media and the potential impact it continues to have on the Trust. Key Performance Indicators may be developed once this policy is embedded further.

## **18. References**

Induction; Recruitment & Selection; Internet Use Policy and Personal Use by Staff of Social Media Policy.

## **19. Associated Documents**

Dignity at Work Policy; Disciplinary Policy (Managing Conduct and Performance); Digital Communications Strategy; Use of Photography CSOP 2.3

## Appendix A – Checklist for the Development or Review and Approval of Procedural Document

	Title of document being reviewed:	Yes/No/ N/A	Comments
<b>1.</b>	<b>Purpose</b>		
	Are the reasons for the development of the Document stated?	Yes	
<b>2.</b>	<b>Definitions</b>		
	Have all key terms been clearly defined?	Yes	
<b>3.</b>	<b>Consultation</b>		
	Have relevant stakeholders and/or users been consulted with?	Yes	
<b>4.</b>	<b>Equality Impact Assessment</b>		
	Has the Trust Equality Impact Assessment Screening Form been completed and attached by the author and approved by the responsible Executive Director?	Yes	Completed, but ED sign off to happen prior to EMT sign off
<b>5.</b>	<b>Monitoring</b>		
	Has the Monitoring Table been fully completed and attached?	Yes	
<b>6.</b>	<b>References/Associated Documents</b>		
	Are key references cited?	Yes	
	Are linked documents identified where appropriate?	Yes	
<b>7.</b>	<b>Approval</b>		
	Does the Document identify which committee/group will approve it?	Yes	SPF then EMT
<b>8.</b>	<b>Dissemination and Implementation</b>		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
<b>9.</b>	<b>Review Date</b>		
	Is the review date identified?	Yes	As standard to new policies

<b>Information Governance Lead (or delegated authority)</b>			
This Procedural Document complies with the Policy for the Development of Procedural Documents			
Name		Date	
<b>Clinical Quality Team</b>			
The Procedural Documents complies with the relevant NHSLA standards			
Name		Date	
<b>Please attach to the procedural document and forward to the relevant committee for approval</b>			

Use of Social Media and/or Networking Sites Policy

**Appendix B – Monitoring Table**

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
<i>Impact on ER casework</i>	<i>HR Business Partners</i>	<i>Casework tracking sheet</i>	<i>Monthly</i>	<i>No. of social networking investigations taking place and successful outcomes</i>	<i>Sent for review by Associate Director of HR</i>	<i>Regional HR Meeting</i>	<i>Referral to HR Policy group for formal policy review + then ratification through SPF</i>

**Appendix C**

**Equality Impact Assessment: Executive Summary**

<b>Executive Summary Page for Equality Impact Assessment:</b>	
Document Reference:	Document Title: Use of Social Media and/or Networking Sites Policy
Assessment Date: 13 November 2012	Document Type: HR Agreement
Responsible Director: Christina Youell	Lead Manager: Tracey Leghorn
Conclusion of Equality Impact Assessment:	
Recommendations for Action Plan:	
Risks Identified:	
<b>Approved by a member of the executive team:</b>	
<b>YES</b>	<b>NO</b>
Name:	Position:
Signature:	Date:
<b>This whole document should be stored with the master document and a final approved electronic copy must be sent to the Equality &amp; Diversity Lead at Bedford Office</b>	