London Ambulance Service NHS

NHS Trust

Policy for Use of Social Media

DOCUMENT PROFILE and CONTROL.

Purpose of the document:

To help staff understand their responsibilities when using social media and the legal implications involved; and to illustrate where problems can arise for individual staff members and the Service.

.

Sponsor Department: Communications

Author/Reviewer: Communications Manager. To be reviewed by January 2020

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
27/09/2017	3.2	IG Manager	Formatting and Document Profile and Control update
04/09/2017	3.1	Head of Media	Additional wording added from LSMS as required by PMAG
19/01/2017	2.6	Head of Media	Amendments
8/11/2016	2.5	Head of Media	Amendments
16/06/2016	2.4	Senior HR Manager	Amendments
19/06/2015	2.3	IG Manager	Document Profile and Control update
21/05/2015	2.2	Comms manager	Minor amendments
28/06/2013	2.1	IG Manager	Document Profile and Control update
07/06/2013	1.3	Head of Comms	Amendments based on Beachcroft, HR and SMT feedback.
17/12/2012	1.2	IG Manager	Document Profile and Control update, new Implementation Plan and formatting changes.
14/12/2012	1.1	Head Comms	Amendments requested by SMG following Approval.
8/11/2012	0.6	Head Comms	Amendments incorporated from ADG meeting on 31 October 2012
24/10/ 2012	0.5	Head Comms	Amendments incorporated from ADG meeting on 27 June 2012
20/06/2012	0.4	Head Comms, Web Officer and Comms Manager	Amendments incorporated from members of ADG, Information Governance Group, Director of Health Promotion and Quality
15/03/2012	0.3	Head Comms, Web Officer and Comms Manager	Further amends and additional content
23/02/2012	0.2	Head Comms	Initial amendments and comments on first draft
November 2011	0.1	Web Officer and Comms Manager	

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	Date Approved	Version
PMAG	26/01/17	3.0
EMT	12/06/2013	2.0
SMG	14/11/2012	1.0
Ratified by (If appropriate):		

Published on:	Date	By	Dept
The Pulse (v3.2)	28/09/17	Digital Media Officer	Comms
The Pulse (v2.3)	22/06/15	Governance Administrator	G&A
The Pulse (v2.1)	28/06/13	Web Communications Officer	Comms
The Pulse	18/12/12	Governance Co-ordinator	GCT
LAS Website (v3.2)	28/09/17	Digital Media Officer	Comms
LAS Website (v2.3)	22/06/15	Governance Administrator	G&A
LAS Website (v2.1)	28/06/13	Web Communications Officer	Comms
LAS Website	18/12/12	Governance Co-ordinator	GCT
Announced on:	**Date**	**By**	**Dept**
The RIB	03/1017	IG Manager	IG
The RIB	02/07/13	IG Manager	GCT
The RIB	18/12/12	IG Manager	GCT

Equality Analysis completed on	By
10/12/12	Head Communications
Staffside reviewed on	**By**

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1. Introduction

Social media is a term commonly used for web-based tools available on the internet that allow people to interact with each other in some way by sharing information, knowledge, opinions and interests.

Examples of social media sites include:

- Social networking sites (eg Facebook, Google+, LinkedIn)
- Micro-blogging sites (eg Twitter)
- Blogs and personal websites
- Messaging boards
- Bookmarking websites (eg del.icio.ous)
- Photo and video content sharing sites (eg Instagram, YouTube, Vimeo, Pinterest and Flickr)

This list is not exhaustive as social media is a constantly evolving area and the types of social media available may change over time.

The Service allows access to Facebook from work computers for all staff. Other social media sites are restricted and not everyone will have direct access. However, the communications team is working with IM&T to open up access to more channels to enable more information sharing. The majority of staff access social media sites on personal devices such as smart phones.

When a member of staff identifies that they work for the Service and/or discusses their work on a social networking site, they must behave professionally and in a way that respects confidentiality and protects patients, members of the public, work colleagues and the reputation of the London Ambulance Service.

Once someone uses social media then what they say is in the public domain – the same personal considerations which govern individuals' general communication should also apply to social media. The general advice is that if a member of staff has doubts about the appropriateness of posting about a particular issue on social media then it is best that they do not do so or they seek advice from a manager or member of the communications team. The Health & Care Professions Council advises its members to 'apply the same standards of behaviour as you would elsewhere. If you wouldn't put something in a letter or email or say it out loud, don't say it on social media.'

2. Scope

This policy applies to all staff who are directly employed by the Service. It also applies to any agency workers, students and volunteers whilst on placement with the Service.

The policy sets out staff's responsibilities when using social media and the legal implications involved. It is not intended to stop members of staff from using social media sites in their own time, but to outline some areas of best practice and illustrate where problems can arise for individual staff members and the Service.

3. Objectives

The objectives of this policy are to enable staff:

- to understand their responsibilities when using social media and what should, and should not, be electronically written or posted
- to highlight the potential risks involved when posting on a social networking site
- to document the Service's intentions for the use of social media
- to understand the implications of using social media inappropriately
- to know where they can go for further advice.

4. Responsibilities

All employees have a responsibility to follow the principles set out in this policy.

Anyone who is found to have breached them may face disciplinary action in line with the Service's disciplinary policy (HR021).

In particular, staff should ensure that they know Service policy on patient confidentiality and follow it at all times.

Registered Healthcare Professionals should be aware of and adhere to the standards and guidelines published by their relevant registering authority, and are advised that they may put their registration at risk if they post inappropriate information on social networking sites. For example the HCPC's Standards of Performance and Ethics sets out the expectations of registrants in terms of their general communication as well as expectations regarding confidentiality and specifically states that 'you must use all forms of communication appropriately and responsibly, including social media and networking websites'. The HCPC has additional advice regarding the use of social media at http://hpc-uk.org/registrants/standards/socialnetworking/
and has draft guidance on confidentiality which is currently out for consultation http://www.hcpc-uk.org/assets/documents/10005192Guidanceonconfidentiality-draftforconsultation.pdf

5. Principles

Social media can blur the boundaries between a person's private and professional lives. Staff who use social media in their personal life should therefore be mindful that inappropriate use, even if it does not mention the Service could damage their own reputation and therefore be of concern to the Service.

When a member of staff identifies their association with the Service – for example, by stating they work for the Service or posting pictures of themselves in uniform or at work - and/or discusses their work, they are expected to behave in line with the highest standards, and in a way that is consistent with the organisation's values and policies.

Even if a staff member does not directly associate themselves with the Service, their link with the organisation can become known through images on friends' sites or on the Service website, or by someone searching for names via internet search engines.

When using any social media channel staff should follow the principles outlined below.

5.1 Only use social media in your own time

Staff should refrain from usingsocial media sites during their working hours unless they are on a break Use of personal devices to access social media sites should be limited to allocated break times.

5.2 Make clear opinions are your own

If a member of staff discloses that they work for the Service or can be identified as an employee through association with other people, they should ensure their profile and related content is consistent with how the Service would expect them to present themselves to colleagues and business contacts.

Staff should also make it clear that their views are their own, not those of their employer.

The use of a disclaimer, however, does not override the need to follow other principles in this policy.

5.3 Do not set up official Service sites

All official social media sites are managed by the communications department. The communications department also endorses other official Twitter accounts. These are run by staff who are trained to act as official spokespeople for the Service. They are subject to separate rules and guidance and receive regular training and updates.

No other teams/staff within the Service should set up corporate sites without the authorisation of the communications department.

Nor should staff not set up sites that are made to resemble an official site.

5.4 Communicate as yourself

If a member of staff associates themselves with the London Ambulance Service, or can be reasonably identified as a member of the London Ambulance

Serviceon their social media site, they are expected to post under their real name. This demonstrates openness, honesty and accountability.

If an employee posts under a pseudonym and at a later stage these posts are associated with their real name, all previous posts will be admissible in a disciplinary investigation or hearing.

5.5 Respect others

Where a member of staff is associated with the Service, or is identified as an employee of the Service, they must not posts anything that is disparaging about a group or individual concerning for example their lifestyle, culture or their social or economic status . as well as the characteristics protected by law – age, disability, gender reassignment, race marriage and civil partnership, pregnancy and maternity, religion or belief, sex and sexual orientation.
Staff should seek permission from colleagues before posting personal details or images that may link their colleague with the Service and should not post anything about someone if they have been asked not to. Staff must always remove information about a colleague if they have been asked to do so.

5.6 Be aware of how online posts are, or can become, public

When staff publish something on social media, they should assume it is in the public domain.

Staff should be aware of privacy limitations when posting material. Even if something is initially shared with a limited group of followers or friends, it could still be copied and shared or published elsewhere.

Staff should carefully consider what they want to say before they publish anything, and work on the basis that anything they write or post could be shared more widely without their knowledge or permission.

Staff should configure their privacy settings and review them regularly because:

- social media sites cannot guarantee confidentiality, and do change settings
- the public, employers or any organisation staff have a relationship with may be able to access their personal information
- once information is online, it can be difficult if not impossible to remove it.

Staff should be careful when sharing or retweeting posts, as they could be seen to be endorsing someone else’s point of view.

A member of staff’s ignorance of the workings or boundaries of a social media tool will not be considered as justifying a breach of this policy. Guidance is available from the communications team if any member of staff is concerned about their privacy settings.

Similarly, whilst all relevant factors will be taken into consideration, reliance on any underlying medical condition to explain or justify inappropriate use of social media will not, of itself, absolve the staff member from responsibility.

5.7 Get your facts right

When posting information, staff must ensure it is factually correct. If they discover they have reported something incorrectly, they should amend it and make it clear they have done so.

5.8 Ensure comments are legal

All comments must be legal and must not incite people to commit a crime.

5.9 Understand the implications of defamation

Staff could face legal proceedings for posted comments aimed at named individuals or an organisation that are considered to harm reputation.

5.10 Respect copyrights

Staff must not use the Service's crest or the NHS logo anywhere on their social media sites, or copy photos from the Service's internet or intranet sites and pass them off as their own – these are copyright protected.

5.11 Be careful when talking about work-related issues

Staff should only share information about the Service that is in the public domain, and should not add derogatory comments on these issues.

Staff must also respect patient confidentiality, and should not disclose information that could identify a patient. See section 5.14 – Protect patient confidentiality.

5.12 Don't bring yourself or the Service into disrepute

Staff should not air grievances or publish anything that risks bringing the Service into disrepute.

5.13 Be careful about the use of photos

Staff should think carefully before posting photos that relate to their work. If staff post any photos of themselves or colleagues in uniform, or in an identifiable work setting, they must ensure that these represent a professional image of the Service. Staff should not use a photo of themselves in uniform as their profile picture; this could give the impression that their site is an official site.

Staff must not post images containing patients on personal social media accounts that could identify the patient or lead the patient to identify themselves.

They should also not post images of a patient's injuries or clinical records (for example, patient report forms, electrocardiograms (ECGs), screen grabs of MDTs, X rays or pictures of any incidents they have attended that could identify the patient or lead the patient to identify themselves. This does not prevent staff sharing, retweeting or linking to images that have been published on official Service sites.

5.14 Protect patient confidentiality

Confidentiality must be respected by anyone who posts anything about their work on the internet, and under no circumstances should anything be posted that identifies a patient.

Staff should ensure they know Service policy on patient confidentiality and follow it at all times.

The DH guidance on patient confidentiality is contained in the publication "Confidentiality: NHS Code of Practice (Nov 2003)".

It states that all NHS staff have a duty to keep confidential all information about patients, and to not disclose this information to anyone not involved directly in their care. It is a legal obligation derived from case law; a requirement within professional codes of conduct; and is included in NHS employment contracts as a specific requirement linked to disciplinary procedures.

It is generally accepted that information provided by patients to the health service is provided in confidence and must be treated as such so long as it remains capable of identifying the individual it relates to. Once information is effectively anonymised it is no longer confidential.

Whilst there are no clear obligations of confidentiality that apply to the deceased, the Department of Health and the General Medical Council agree there is an ethical basis for requiring that confidentiality obligations must continue to apply.

It is Service policy to gain written consent from patients for all disclosures of identifiable information to the media and for publicity purposes. As well as names and other personal details, this includes the use of images of the patient undergoing treatment in a real life situation and where the patient is posing for a picture; and the release of taped 999 calls.

The following is patient-identifiable information and should not be disclosed:

- Patient's name, address, full postcode or date of birth
- Pictures, photographs, videos, audio-tapes or other images of patients
- NHS number and local patient identifiable codes
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

The DH definition of anonymised information is “information which does not identify a patient directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combinations of details that might support identification.”

Indirect breaches of confidentiality

Nothing written by staff should comment on, or provide additional information about, cases already in the public eye – for example, any incident that has already been reported in the media.

While individual pieces of information may not alone breach patient confidentiality, the sum of published information online could be sufficient to identify a patient.

In cases where an incident becomes public knowledge after information has been posted, the member of staff should consider whether the published details could now be considered to be breaching the patient’s confidentiality and, if so, remove them.

5.15 Respect safeguarding issues

Posts made by staff must not encourage behaviour that could be linked to safeguarding issues, for example:

- Bullying
- Luring and exploitation
- Theft of personal information
- Encouraging self harm or violence
- Glorifying activities such as excessive drinking or drug taking

These kinds of posts may be investigated and result in disciplinary action.

5.16 Adhere to other Service policies and procedures

Staff using social networking sites should always adhere to the Service’s vision and values, as well as codes of conduct and policies which are part of their professional and employment requirements. These include:

- Professional code of conduct (eg Health & Care Professions Council)
- Guidance on social media (Health & Care Professions Council)
- Other codes of conduct (eg confidentiality clause in your contract)
- The LiA Facebook code of conduct
- Relevant trust policies, including:

  TP024 – Managing patient confidentiality when dealing with the media
  TP031 – Internet policy
  TP060 Policy for acceptable use of IT systems
  TP003 – Policy statement of duties to patients

HR/09/02 – Disciplinary policy
Equality and inclusion policy

5.17 Security alerts concerning individuals posing a threat to the Service or its staff

Occasionally NHS staff are made aware of individuals who may pose a threat to the Service or its staff. For their safety, information is shared with staff to protect them as they go about their duties. Disclosure of information within an alert, or the alert itself, should not be made to non-NHS staff/contractors or organisations (other than Police or Crown Prosecution Service), without first consulting the Local Security Management Specialist, located in the Health, Safety and Security department – Unless there is an imminent threat to persons or an offence being committed and it is not practicable to obtain advice or consent. Any disclosures also need to be documented including the reasons for the disclosure. For this reason it is not appropriate to share details of any security alerts. Further advice is available from the security manager.

6. Profiting from social media

Staff may accept payment or other inducement for their own material produced away from their London Ambulance Service employment, provided that it has been officially registered and sanctioned as a business interest, and providing the material does not in any way relate to ambulance service work.

Applications to carry out any such work should be done by applying the Service's Second job policy (HR/001)

7. Staff with authorised access to social media sites for work purposes

The use of social networking sites is not normally permitted from Service computers, and most of these sites are restricted by the Service's web filtering software, managed by IM&T.

Some staff will be authorised to access social media sites either for monitoring purposes, or to post information on behalf of the Service.

Staff who are given access to social media sites such as YouTube, Twitter and Facebook for work purposes must:

- only use these sites in an ethical and lawful manner – subject to the same principles as above, such as patient confidentiality, not bringing the Service into disrepute and not posting sensitive information.
- not access their personal accounts – such as Facebook, Twitter and blogs, unless it is for the benefit of the Service

- make total separation between their personal accounts and any accounts monitored or updated on behalf of the Service.

8. Being harassed, bullied or victimised via a social networking site?

If staff believe they are being harassed, bullied or victimised as a result of another member of staff's post to an internet site, they can take action. Staff should access the Service's Dignity at work policy (HR026)which outlines the informal and formal action that can be taken.

Alternatively, they can inform their line manager or an adviser in HR, or report the incident to the police or to the social media site.

9. Misconduct

Any member of staff found to be using social media sites inappropriately, as outlined in the principles above, may be subject to disciplinary action and will be managed in line with the Service's disciplinary policy (HR/09/02).

Those registered with professional bodies including clinicians are reminded that they may put their registration, and therefore their employment, at risk if they post inappropriate information on social networking sites.

10. Further information

Any staff who are in any doubt about what they should or should not post on social media sites – particularly about their work – or who discover online content that may harm the reputation of the Service, should contact the communications department by email to discuss the matter or raise their concerns via:

communications@londonambulance.nhs.uk

If a member of staff is contacted by the media about anything Service-related they have written or to request other information or an interview, they should contact the communications department.

11. The Service's use of social media

The Service uses social media as part of its communication strategy. The communications department has authority to speak on behalf of the Service and is responsible for managing the Service's official sites, including Facebook, Twitter, YouTube and Instagram.

Social media, like other communication tools, is used to improve the public's understanding of the Service and its work, promote health, and engage with the general public.

When using social media sites, the communication department and those authorized by the communications department, will, on behalf of the Service, ensure it:

- is respectful towards patients, members of the public and Service employees
- does not reveal confidential or sensitive information about patients, staff or the Service
- is transparent
- updates the channels on a regular basis and respond to users posts
- removes any content posted by other users that is considered offensive or derogatory.

The communication team adheres to the policies and procedures listed at 5.16 when using social media.

Sources/references

BBC Guidance – Social Networking, Microblogs and other Third Party websites: Personal Use (October 2010)
Chartered Institute of Public Relations (CIPR) Social Media Best Practice Guide (May 2011)
Norfolk and Norwich University Hospitals NHS Foundation Trust Policy on personal use by staff of social media (September 2010)
Metropolitan Police Service guidance to officers and staff on use of social media
London Fire Brigade – ICT acceptable use policy (18 April 2012)
Cabinet Office – Social media guidance (17 May 2012)
HCPC – social media guidance (http://www.hpc-uk.org/Assets/documents/100035B7Social_media_guidance.pdf)
Royal College of General Practitioners – Draft social media highway code ((27 September 2012)
Nursing & Midwifery Council – Social networking sites. The use of social networking sites by nurses, midwives and students (Online – http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/ - June 2012)
General Medical Council – Doctors' use of social media. A draft for consultation
Royal College of Nursing – Legal advice on using the internet (October 2009)
Rotherham Doncaster and South Humber NHS FT – Policy relating to employee usage of social media (29 February 2012)
Gloucestershire Constabulary – Guidance to all staff from the Professional Standards Department on social media
Sussex Police – Social Media Policy (2012)
HCPC Standards of performance, conduct and ethics (2016)

<table>
<tr><th colspan="5">IMPLEMENTATION PLAN</th></tr>
<tr><td><b>Intended Audience</b></td><td colspan="4">For all LAS staff</td></tr>
<tr><td><b>Dissemination</b></td><td colspan="4">Available to all staff on the Pulse</td></tr>
<tr><td><b>Communications</b></td><td colspan="4">Guidelines to be announced in the RIB and a link provided to the document</td></tr>
<tr><td><b>Training</b></td><td colspan="4">No training is required</td></tr>
<tr><td colspan="5"><b>Monitoring:</b></td></tr>
<tr><td><b>Aspect to be monitored</b></td><td><b>Frequency of monitoring
AND
Tool used</b></td><td><b>Individual/ team responsible for carrying out monitoring
AND
Committee/ group where results are reported</b></td><td><b>Committee/ group responsible for monitoring outcomes/ recommendations</b></td><td><b>How learning will take place</b></td></tr>
<tr><td>Whole policy.</td><td>To be initially reviewed after three months</td><td>Head of Communications.
To be reported to SMG.</td><td></td><td></td></tr>
</table>