Essex Partnership University
NHS Foundation Trust

SOCIAL MEDIA PROCEDURE

PROCEDURE NUMBER:	CPG58
VERSION NUMBER:	1
AUTHOR:	Associate Director of Communications
CONSULTATION:	
IMPLEMENTATION DATE:	January 2018
AMENDMENT DATE(S):	N/A
LAST REVIEW DATE:	January 2018
NEXT REVIEW DATE:	January 2021
APPROVAL BY EOSC:	16 January 2018
APPROVAL BY FINANCE & PERFORMANCE COMMITTEE:	25 January 2018

SCOPE

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is the Executive Director of Corporate Governance & Strategy

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SOCIAL MEDIA PROCEDURE

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SOCIAL MEDIA PROCEDURE

Assurance Statement

This procedure outlines the Trust's arrangements for the use of social media in order to ensure that staff are clear about the processes and procedures for using social media on Trust or personal computers. This procedure supports and underpins the Trust Social Media Policy.

1.0 INTRODUCTION

1.1 The Trust's Social Media Policy ("the Policy") governs the publication of and commentary on social media by employees of EPUT.

1.2 This is the Trust's Social Media Procedure ("the Procedure") which sets out what steps an employee must take when engaging in any social media to which the Policy applies. This Procedure should be read in conjunction with the Policy.

2.0 SETTING UP SOCIAL MEDIA

2.1 Social media identities, logon ID's and user names may not use EPUT's name without prior approval from the Communications Team. This particular prohibition applies to both Business Related Use and Personal Use (as defined in the Policy).

2.2 Some social networks require a photo or avatar in order to complete a profile. Where a photo is required, and where the intended use of the social media is business related use, Trust approved photographs must be used for your profile photograph. Approved photographs can be obtained from Communications Team.

2.3 If you are engaging in social networking on behalf of the Trust or a Trust group/event (which, for the avoidance of doubt, includes any business related use), your profile on social media sites must be consistent with your profile on the EPUT website or other EPUT publications. If in doubt, staff must contact the Communications Team for an approved corporate profile.

2.4 Staff interested in using social media on behalf of the Trust or for a Trust group/event must complete the Social Media Request Form (Appendix 1). This form must be endorsed by a senior manager and returned to the Communications Team. Once the request is approved by the Associate Director of Communications, the Communications Team will assist in the creation of the requested social networking account.

3.0 CONFIDENTIALITY

3.1 While it is acceptable to discuss and/or write about your work and have a dialogue with the community it is unacceptable to publish confidential and/or personally identifiable information.

3.2 Confidential information includes information that is considered 'sensitive' or protected from release under the Freedom of Information Act 2000 (FOI). Confidential information is also anything which may be held within patient health records; staff (Human Resource) records, financial / other corporate records.

3.3 Person-identifiable information is anything that contains the means to identify a person, such as:

- Name
- Address
- Date of birth
- Postcode
- NHS number
- NI number
- Visual images (e.g. photographs that could identify an individual)

3.4 In all online interactions staff must respect the wishes of our patients/service users and of their colleagues in keeping their personal information private. Staff must also be mindful not to place the organisation in a detrimental position.

3.5 Staff must refer to the Trust **Procedure on Confidentiality CPG59b / Information Governance and Security Policy CP50.**

4.0 PRIVACY SETTINGS

4.1 Privacy settings on social media platforms should be set to allow anyone to see profile information similar to what would be on the EPUT website. Be mindful of posting information that you would not want the public to see. Other privacy settings that might allow others to post information or see information that is personal should be set to limited access.

5.0 RESPONSIBLE USE OF SOCIAL MEDIA

5.1 This section of the Procedure provides staff with common-sense guidelines and recommendations for using social media responsibly and safely where the Policy applies.

5.1.1 **Honesty and Openness**
Staff engaging in social media on behalf of the Trust or any affiliated groups or events are not permitted to use the medium anonymously, using pseudonyms or false screen names. The Trust is committed to transparency and honesty in all its dealings.

Staff must use their real names – be clear who you are, and identify that you work for EPUT. It is important to be thoughtful and appropriate in all communications. Anything published via social media may be considered permanent information, stored on the Internet for perpetuity, even after the message is deleted. Therefore, it is important that staff consider the content of all communications carefully and be cautious about disclosing their own personal details.

It is important that when engaging in social networking, staff are upfront and honest if an error or misinterpretation is made.

5.1.2 Protecting the Trust's Reputation

Where staff members identify themselves as employees of the Trust, they must state that their views do not represent those of the Trust unless the postings they make are specifically authorised by the Trust. For example, staff could state, "the views in this posting do not represent the views of EPUT". Staff should also ensure that their profiles and any content posted are consistent with the professional image staff members present to colleagues and service users.

Staff members should avoid posting comments about sensitive business-related topics, such as the Trust's performance. Even if staff members make it clear that their views on such topics do not represent those of the Trust, their comments could still damage the Trust's reputation.

If staff members are uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they discuss it with their line manager.

If staff members see content in social media that disparages or reflects poorly on the Trust or its stakeholders, they should contact the Communications Team. All staff are responsible for protecting the Trust's reputation.

5.1.3 Respecting Intellectual Property and Confidential Information

Staff should not do anything to jeopardise the Trust's confidential information and intellectual property through the use of social media.

In addition, staff should avoid misusing the intellectual property of other companies, organisations or individuals, which can create liability for the Trust, as well as the individual staff member.

Staff members should not use the Trust's logos, brand names, slogans or other trade marks, or post any of the Trust's confidential or proprietary information without prior written permission from the Associate Director of Communications.

To protect staff members and the Trust against liability for copyright infringement, staff members should, where appropriate, reference sources of particular information they post or upload and cite them accurately. If staff members have any questions about whether a particular post or upload might violate anyone's copyright or trademark, they should ask the Trust's legal department before making the communication.

5.1.4 Respecting colleagues, service users and others

Staff must not post anything that their colleagues or the Trust's service users, business partners, suppliers, vendors or other stakeholders would find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything related to their colleagues or the Trust's service users, business partners, suppliers, vendors or other stakeholders without their written permission.

Staff must consider the potential consequences prior to communicating via social media. Staff must be tactful when publishing negative opinions even if they are true. The Trust's staff, service users and membership community reflect a diverse set of customs, values and points of view. It is therefore important not to communicate information about the Trust which is contradictory or in conflict with the EPUT website.

Proper consideration must be given to privacy and to topics that may be considered objectionable or inflammatory – such as politics and religion. Use your best judgment and be sure to make it clear that the views and opinions expressed are yours alone and do not represent the official views of EPUT.

Social Media should not be used for the purposes of stalking or making / receiving unwanted contact and that privacy settings should be adjusted appropriately. Staff should not be adding service users to their contacts and a professional boundary must be maintained and respected at all times.

5.1.5 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' normally involves raising the issue internally in the first instance. The Trust's **Whistleblowing Policy HR12** sets out the various means of raising concerns. Using social media to whistleblow without already having raised concerns through the proper channels would not be considered appropriate and may not be supported by the Trust.

6.0 SOCIAL NETWORKING GUIDELINES

6.1 Facebook Guidelines

- If the primary audience of your communication is public, then request to create a 'Fan' Page.
- If the primary audience of your communication is internal to the Trust (i.e. colleagues) or a specific target group (i.e. members of a specific stakeholder organisation/group), then request to create a Group.
- Do not attempt to create 'personal' pages for official Trust groups or event.
- The requester or organiser will be primary administrators for all Facebook Groups and Pages. In certain circumstances the communications team will be primary administrator.
- Approved Facebook Groups or Pages will be checked regularly and any found to be violating the principles in sections 3.0 – 5.0 above will be terminated immediately and action taken as appropriate against the 'Requester' and/or 'Organiser'.

6.1.1 Facebook Groups and Facebook Pages

- Groups are meant for organising on a personal level and specific interaction around a cause (i.e. Race 4 Life).
- Groups are set up to allow for more personal interaction between members.
- Groups can be set to public, private or 'secret', giving administrators control over membership and visibility of posts.
- Group administrators can send messages directly to all members of the group

6.1.2 Facebook (Fan) Pages

- Facebook pages are better for Trust related Groups (i.e. Wellbeing Festival) and Campaigns (i.e. Make A Difference).
- Facebook pages act as an entire corporate entity. Connections are 'Fans' not 'Friends'.
- Pages 'liked' by an individual show up on that individual's personal Wall, where friends/the public can see them and follow the links. Pages are always public.
- Page administrators cannot send messages directly to all fans of the page
- Page administrators can create general 'Updates' that appear in a specific Updates section of the personal pages of all fans.

6.1.3 Facebook Groups and Facebook Pages

- Facebook Events can be created using either group or fan page accounts.
- Both groups and fan pages are indexed by search engines such as Google. It is important to be aware that all content can be 'found' in search engine results.
- Both groups and pages can be searched within Facebook if the group setting is public.

6.2 **Twitter Guidelines**

- Twitter is the most appropriate social network to deliver short messages with a link to a website for further information. Twitter is not the most appropriate medium if there is no website to direct readers to for further information.
- All Twitter messages have a limit of 140 characters, which includes all punctuations and spaces. It is therefore important that Twitter messages are kept brief, to the point and yet comprehendible.
- The requester or organiser will create their own Twitter account and be the primary administrator.
- Approved Twitter accounts will be checked regularly and any found to be violating the principles in sections 3.0 – 5.0 above will be terminated immediately and action taken as appropriate against the 'Requester' and/or 'Organiser'.

7.0 COMPLIMENTS AND COMPLAINTS

7.1 If a member of the public raises an issue via any social media platform which would usually be dealt with by the Patient Advice and Liaison Service (PALS), such as questions about referrals into EPUT services, or requests for information or advice about a specific service, then staff can respond stating that that such queries can be directed to our PALS Dept.

7.2 Staff are not to engage or respond to queries which would usually be dealt with by PALS.

7.3 If a member of the public raises a concern or makes a complaint about anything related to the Trust, its services, its staff or any of its related activities, it is important for staff not to engage or respond directly to the concern or complaint but refer the individual to the Complaints Dept in the same manner as above.

7.4 The Complaints and PALS Departments will respond and deal with all queries, concerns or complaints that come in via social media in accordance with the **Complaints Policy CP2**.

8.0 MONITORING AND ENFORCEMENT

8.1 Access to the Internet will be inspected and / or monitored by Trust systems to protect the Trust, Trust Computing Facilities and account holders from internet / electronic mail borne viruses / macros / inappropriate attachments and / or content by the IT Department where possible. Staff are not permitted to use the Trust's IT resources and communications systems for any matter that you wish to be kept private or confidential from the Trust.

8.2 The Communications Team will monitor use of the Trust name, logo and other branding on the Internet. Any unauthorised use of the Trust name, logo or other branding will be reporting using established incident reporting mechanisms.

8.3 The Information Governance team will analyse any incident reports and trends. Any recognised trends will be reported to the Executive Team who may deem that further investigation is necessary.

8.4 Line Managers will monitor individual staff conduct and report any issues of concern in order that further action may be taken if necessary.

8.5 Staff who violate this Procedure and the associated Policy may be subject to disciplinary action in accordance with the Trust's **Conduct & Capability Policy HR27B**.

9.0 RELATED POLICIES AND PROCEDURES

- Social Media Policy
- Procedure on Confidentiality
- Information Governance and Security Policy
- Complaints Policy
- Conduct & Capability Policy

END