Essex Partnership University
NHS Foundation Trust

Freedom of Information Request

Reference Number: EPUT.FOI.19.1106
Date Received: 6 June 2019

Information Requested:

1. Do you have a staff social media policy?
   The Trust has a staff Social Media policy.

2. Do you have a policy or guidance on staff use of messaging apps, such as WhatsApp, Siilo, Forward?
   Essex Partnership University NHS Foundation Trust is currently drafting Instant Messaging protocol for staff.

3. Does your Trust actively discourage the use of WhatsApp?
   Yes.

4. In the past two calendar years, have any staff been formally disciplined for the inappropriate use of messaging apps at work (ie for sharing clinical information) or for using unapproved messaging apps? If yes, how many?
   Yes > 5.

   The Trust is unable to provide the specific figures you have requested as these are few meaning there is a risk that these individuals could be identified. Therefore the Trust believes this is exempt under Section 40 (Personal Information) of the Act.*

5. Are you aware how many staff use WhatsApp for work-based communication with colleagues? If yes, how many?
   No.

6. Have you recommended or implemented a messaging platform for use across your Trust? If yes, which app or platform do you use?
   Essex Partnership University NHS Foundation Trust is commencing a pilot project using the Forward Health application.

***Exemption: Section 40: Personal information**

(1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.

(2) Any information to which a request for information relates is also exempt information if—

(a) it constitutes personal data which do not fall within subsection (1), and

(b) either the first or the second condition below is satisfied.

(3) The first condition is—

(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the

disclosure of the information to a member of the public otherwise than under this Act would contravene—

(i) any of the data protection principles, or

(ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and

(b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded.

(4) The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject's right of access to personal data).

(5) The duty to confirm or deny—

(a) does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1), and

(b) does not arise in relation to other information if or to the extent that either—

(i) the giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded, or

(ii) by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed).

(6) In determining for the purposes of this section whether anything done before 24th October 2007 would contravene any of the data protection principles, the exemptions in Part III of Schedule 8 to the Data Protection Act 1998 shall be disregarded.

(7) In this section— "the data protection principles" means the principles set out in Part I of Schedule 1 to the Data Protection Act 1998, as read subject to Part II of that Schedule and section 27(1) of that Act;

- "data subject" has the same meaning as in section 1(1) of that Act;
- "personal data" has the same meaning as in section 1(1) of that Act.

Publication Scheme:

As part of the Freedom of Information Act all public organisations are required to proactively publish certain classes of information on a Publication Scheme. A publication scheme is a guide to the information that is held by the organisation. EPUT's Publication Scheme is located on its Website at the following link https://eput.nhs.uk/publication-category/financial-statements-budgets-and-variance-reports/

SOCIAL MEDIA POLICY

POLICY NUMBER:	CP58
VERSION NUMBER:	4
AUTHOR:	Associate Director of Communications
CONSULTATION:	
IMPLEMENTATION DATE:	October 2011
AMENDMENT DATE(S):	May 2014 (Director Change), October 2014
LAST REVIEW DATE:	October 2014 – August 2017
NEXT REVIEW DATE:	August 2020
APPROVAL BY EOSC DATE:	16 January 2018
RATIFICATION BY FINANCE AND PERFORMANCE COMMITTEE DATE:	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 POLICY

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 POLICY

Assurance Statement

Clear arrangements for social media use need to be implemented so staff are clear about what they may post and where they may be in breach. This Policy provides a mechanism through which the Trust can be effective in social media management and provision. The Trust wants to create a climate of openness and dialogue with all stakeholders. This Policy supports a culture of openness and dialogue in the organisation, but also ensures that the reputation and rights of EPUT, its employees, service users and others is protected and that the risk of misrepresentation by social media postings is reduced. The Trust believes that staff, directors and governors and service users should have access to any appropriate communications channels. The Policy sets out a framework to provide this support.

1.0 INTRODUCTION

1.1 This policy governs the publication of and commentary on social media by employees of EPUT. This policy is in addition to and complements any existing or future Trust policies regarding the use of technology, computers, e-mail and the internet.

1.2 EPUT recognises the importance of social media tools in shaping public thinking about the Trust. The Trust also recognises the importance of our employees joining in, and helping to shape industry conversation and direction through blogging and involvement in social media. The Trust encourages our employees to interact knowledgeably, socially and responsibly on social media sites and the internet.

1.3 EPUT employees are able to publish or comment via social media in accordance with this policy.

1.4 This policy does not form part of any EPUT employee's contract of employment and it may be amended at any time.

1.5 This policy should be read in conjunction with the Social Media Procedure ("the Procedure").

2.0 SCOPE

2.1 This policy applies to all EPUT staff, directors and governors (staff, public and appointed).

2.2 For the purposes of this policy, social media means any facility for online publication and commentary, including without limitation: blogs, wiki's, social networking sites such as Facebook, LinkedIn, Twitter, Flickr, and YouTube.

2.3 It applies to the use of social media only where the employee identifies him/herself as an EPUT employee or where the employee publishes, comments on, forwards or otherwise responds to matters relating to the Trust's activities ("Business Related Use"). For the avoidance of doubt, it does not apply where the employee makes an incidental mention of his/her place of employment in a personal blog on topics unrelated to the Trust and any of its activities. The policy applies regardless of whether the social media is accessed using EPUT's IT facilities and equipment or equipment belonging to members of staff, or whether that access is made during work hours or outside work hours.

2.4 Where this policy applies, staff must follow the Procedure.

2.5 Breach of this policy or the procedure may result in disciplinary action in accordance with the Trust's **Conduct & Capability Policy HR27B**. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether the Trust's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with the Trust's investigation, which may involve handing over relevant passwords and login details. In respect of Governors, breach of this policy or procedure appropriate action will be taken in accordance with the Code of Conduct for Governors and Trust constitution.

2.6 Staff / Governors may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

3.0 RESPONSIBILITIES

3.1 The Chief Executive has overall accountability for this policy and will ensure that the Trust meets its statutory duties.

3.2 The Associate Director of Communications will be the Social Media Policy lead in the organisation and is responsible for making sure that this is policy made available to all staff.

3.3 Information Governance will monitor this policy to make sure it is being properly adhered to. They will examine any incidents or risks that may come up, as soon as they know about them.

3.4 Information Governance will regularly monitor how staff use social media and they will report on this to the Executive Team and Board as appropriate.

3.5 Senior managers will make sure that all staff in their teams are aware of and follow this policy. Line Managers must report concerns or any misuse by staff they are responsible for that they are aware of or any contravention of this policy to a senior manager so it can be investigated.

4.0 PROHIBITED COMMUNICATIONS

4.1 Social media should never be used in a way that breaches any of the Trust's other policies. If an internet post would breach any of the Trust's policies in another forum, it will also breach them in an online forum. Employees are prohibited from using social media to:

(a) Breach the Trust's obligations to its regulator, NHS Improvement;

(b) Breach any obligations they may have relating to confidentiality;

(c) Breach the Trust's **Conduct & Capability Policy HR27B**;

(d) Defame or disparage the Trust, its employees, service users, business partners, suppliers, vendors or other stakeholders;

(e) Publish, comment on, forward, or otherwise respond to any material that is obscene, sexually explicit or pornographic in nature, is offensive, or contains ethnic slurs, personal insults or expletives;

(f) Harass or bully other staff in any way;

(g) Unlawfully discriminate against other staff or third parties;

(h) Breach the Trust's **Procedure on Confidentiality CPG9b** or **Information Governance and Security Policy CP50**;

(i) Engage in any communications that are contrary to the Trust's business interests; or

(j) Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

4.2 Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Trust and create legal liability for both the author of the reference and the Trust.

4.3 Employees that engage in prohibited communications will be in violation of this policy and may also be subject to disciplinary action in accordance with the Trust **Conduct & Capability Policy HR27B**.

5.0 PERSONAL USE OF SOCIAL MEDIA

5.1 The Trust recognises that employees occasionally may desire to use social media for personal use at the office or by means of our computers, networks and other IT resources and communications systems. “Personal Use” means use other than where the employee identifies him/herself as an EPUT employee and on matters that do not relate to the Trust’s activities. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted.

6.0 POLICY IMPLEMENTATION

6.1 All staff will be made aware of this policy as part of their local induction to Trust policies and procedures. Questions regarding the content or application of this policy should be directed to Information Governance.

6.2 The Communications Team will disseminate this policy and any future guidance regarding the use of social media via the Intranet and internal communication channels.

7.0. MONITORING COMPLIANCE WITH THIS POLICY

7.1 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.

7.2 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 reported using established incident reporting mechanisms.

7.3 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.

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

8.0 RELATED POLICIES AND PROCEDURES

- Social Media Procedure
- Procedure on Confidentiality CPG9b
- Information Governance and Security Policy CP50
- Conduct & Capability Policy HR27B

END