Frimley Health NHS Foundation Trust

Trust Policy

Internet Policy

Key Points

- The primary use of the Internet is for health care related purposes
- Staff Internet access is not a right; it is a privilege and should be based on work need.
- Staff shall not access or download offensive material or use the Internet inappropriately If they are found to be in breach of it they could be subject to disciplinary action.
- When using social networking sites, blogging, etc., staff must uphold the reputation of their profession and of the Trust. Unless authorised, staff are not permitted to present views on behalf of the Trust
- The Trust reserves the right to monitor Internet usage, and will take reasonable measures to ensure that staff are aware of this.

Version:	3.1
Role of Policy Lead(s):	Head of Information Governance
Role of Executive Lead:	SIRO
Date Approved by Executive Lead:	September 2018
Name of Responsible Committee:	IG Committee
Date Approved by Responsible Committee:	September 2018
Date Approved by Policy Review Group:	November 2018
Date Ratified at Executive Directors meeting:	November 2018
Date Issued:	December 2018
Review Date:	September 2021
Target Audience:	All staff
Key Words & Phrases:	Internet

Version Control Sheet

Version	Date	Policy Lead(s)	Status	Comment
0.1	March 2017	Acting Head of Information Governance		Transferred to new format
1.0	April 2017	Policy Officer	Final	Approved by HEB
2.0	June 2017	IG Officer	Final	Minor changes to text
2.1	July 2018	Information Governance Administrator	Interim	Logo update
3.0	Nov 2018	Policy Manager	Final	Ratified at Executive Directors meeting
3.1	Dec 18	Head of Information Governance	Interim	Addition of following text at 5.7.1: Users can only use trust email for personal use as detailed in the email policy (section 5.15.2.)

Document Location

Document Type	Location
Electronic	Our Place
Paper	Information Governance Office

Related Documents

Document Type	Document Name
Electronic	Email Policy
Electronic	Equality and Diversity Policy
Electronic	Harassment and Bullying Policy

Contents

1 INTRODUCTION

1.1 The Internet is an unregulated environment. The trust will not be liable for any material viewed or downloaded. Use of the Internet must be consistent with this policy and trust's standards of business conduct.

1.2 Any breach of this policy may lead to disciplinary action, withdrawal of facility and possibly termination of employment. Illegal activities may also be reported to the appropriate authorities.

1.3 "A user" for the purposes of this policy includes all employees of the trust as well as contractors, temporary staff, volunteers and third parties that are granted access to trust information assets.

2 SCOPE OF THE POLICY

2.1 The purpose of this policy is to clearly define the permissible use of the Internet by staff at Frimley Health NHS Foundation trust. This policy also applies to individuals who have authorised access to the Internet through PCs owned or managed by the trust.

2.2 For the content of this policy, the Internet is deemed to include:

- trust intranet (internal web pages), World Wide Web (www/nww), and all publicly accessible websites
- NHS.net
- Access to the above via the trust network

2.3 The use of trust email facilities is subject to further detailed rules which are laid down in the trust's Email policy.

3 DEFINITIONS

3.1 **Internet:** a vast computer network linking smaller computer networks worldwide. The Internet includes commercial, educational, governmental and other networks, all of which use the same set of communications protocols.

3.2 **Intranet:** a computer network with restricted access, as within a company, that uses software and protocols developed for the Internet. For example, NHSNET and the trust's own Intranet.

3.3 **Blogging:** is using public websites to write an on-line diary (known as a blog) sharing thoughts and opinions on various subjects.

3.4 **Social Networking:** is the use of interactive web based sites that mimic some of the interactions that occur between people in life. Examples include Facebook.com and Linkedin.com.

3.5 **Offensive Material:** This includes but is not limited to copyrighted, threatening or obscene material. Offensive material is understood to include hostile text, images or recordings relating to gender, race, sex, sexual orientation, religious or political convictions or disability.

3.6 **Streaming:** is the listening or watching of media without the need to download.

4 PURPOSE OF THE POLICY

4.1 The purpose of this policy is to promote good practice in Internet use.

4.2 State the permissible uses of the Internet by all individuals who have been granted access to the Internet from trust computers.

4.3 Provide guidance to staff on appropriate use of the Internet and to define their responsibilities in relation to it.

4.4 To provide guidance to managers on the process to be followed if inappropriate use is suspected.

5 THE POLICY

5.1 Acceptable Use

5.1.1 Access to the Internet from trust computers, is primarily for work related purposes or as required for professional development and training.

5.1.2 Information obtained from Internet sources must be verified before being used for business purposes.

5.1.3 The trust's website is an important marketing and information resource for the trust. Only authorised members of staff will be able to make changes to the trust Internet site; all changes must meet the trust corporate standards.

5.1.4 Staff who join Internet discussion or news groups (or similar) should conduct themselves in an honest and professional manner. Unless they are authorised to do by the nature of their job and responsibilities, they are not permitted to present views on behalf of the trust.

5.1.5 Staff should be circumspect about what they write about the trust, its clients and employees on social networking sites. It is important that staff uphold the reputation of their profession and of the trust.

5.1.6 Staff are responsible for maintaining the security of their individual login and password.

5.2 Unacceptable Use

5.2.1 Users must not attempt to bypass trust web filtering technology; doing so could lead to disciplinary action leading to possible dismissal.

5.2.2 Users must not make or post indecent remarks, proposals or materials on the Internet.

5.2.3 Users shall not solicit emails that are unrelated to business activity or which are for personal gain, shall not send or receive any material which is obscene or defamatory or which is intended to annoy, harass or intimidate another person and shall not present personal opinions as those of the trust.

5.2.4 Users are not permitted to access, display or download from Internet sites that contain offensive, obscene, hateful or other objectionable material. To do so is considered a serious breach of trust security. The definition of "offensive" will take account of the trust's Equal Opportunity and Bullying & Harassment policies and includes hostile text or images relating to gender, ethnicity, race, sex, age, sexual orientation, religious or political convictions or disability.

5.2.5 Users may not upload, download or otherwise transmit commercial software or any copyrighted materials belonging to the trust or any third parties without prior permission.

5.2.6 Use of the Internet for commercial activities other than in the conduct of the Frimley Health NHS Foundation trust business is prohibited.

5.2.7 Users must not share their username or password with anyone (this is a direct breach of the Computer Misuse Act 1990). If a breach of security is recorded under a user's login the burden of proof will be with that user to show that, as the named user, they are not responsible for the breach.

5.2.8 If the trust should be brought into disrepute, be embarrassed or be damaged financially or otherwise as a result of something written about it by an employee, that individual would be subject to disciplinary action and possibly dismissal.

5.3 **Copyright**

5.3.1 Much of the information that appears on the Internet is protected by copyright. Unauthorised copying or modifying, copyright protected material, including software, breaches copyright law. Therefore, downloading software or copyright protected information is not permitted as it may make you and/or the trust liable to legal action.

5.4 **Trust Wireless Internet**

5.4.1 Patients and visitors to the trust are able to access the Internet via the trust's wireless network. All users must accept terms and conditions prior to accessing the trust wireless network. The trust will prohibit users to access illegal sites.

5.5 **Use of Intranet**

5.5.1 The trust intranet is an internal communication that is used for the communication and management of trust information.

5.5.2 Certain members of staff will be granted access to upload information onto the trust intranet. Staff provided with this privileged access must ensure when uploading information they comply with all relevant trust policies and procedures.

5.5.3 The technical management and creation of the trust intranet has been delegated to the trust's Communications team and the trust's Digital communications manager.

5.6 **Access to Prohibited Websites (Black Listed)**

5.6.1 The trust has put in place technical measures to restrict access to all internet sites that are recommended for restriction to meet industry standards or in line with Department of Health list of prohibited websites. The banning of these websites is to protect the security and reputation of the trust and its IT systems and networks.

5.6.2 This list is dynamic and may be updated at any time to reflect changes in guidance or legislation.

5.6.3 Where a website is hosting known illegal or questionable content, the trust will not action any change to make the website available to a requesting staff member.

5.7 **Personal Use**

5.7.1 Staff may only use the Internet for personal use where the following conditions apply:

- Undertaken within approved breaks or outside of working hours

- Does not interfere with the performance of their duties at work
- Users can only access sites in line with this policy
- User must not arrange for any goods ordered on the Internet to be delivered to the Company address (excluding the Amazon boxes) or order them in the Company's name.
- Users can only use trust email for personal use as detailed in the email policy section 5.15.2.

5.7.2 The trust will take no responsibility or liability for any loss of credit or debit card (or other financial) details, which a user may disclose while using the Internet. Individuals are advised not to supply these details; however, if they choose to do so, this is entirely at their own risk.

5.8 **Monitoring Individual Users**

5.8.1 All staff internet activity will be monitored and logged. Where a member of staff's Line Manager believes that a member of staff is accessing the Internet in breach of this policy, the Line Manager can request a report on the member of staff's usage. Reports will be undertaken in full consideration of Article 8 of the Human Rights Act 1998 and the Information Commissioners Office "The Employment Practice Code: Part 3 Monitoring at Work"

5.9 **Removal of Internet Access**

5.9.1 Where, upon monitoring staff usage of the internet, it is established that usage is inappropriate or excessive, the trust reserves the right to withdraw internet access from the member of staff.

5.9.2 Where this is the case, the trust will notify the member of staff in writing in full liaison with the trust's HR Department.

5.9.3 In exceptional circumstances, a Manager may request a member of staff's internet access is removed (this may or may not be part of a disciplinary action), if having access to the internet is not a requirement of their role. The request of the Manager would be undertaken in full consultation with the HR Department.

6 DUTIES/ ORGANISATIONAL STRUCTURE

6.1 **The Chief Executive will:**

6.1.1 Ensure that this policy is fully implemented and monitored.

6.2 **Managers will:**

6.2.1 Ensure that all of their staff are aware of this policy and understand their responsibilities.

6.2.2 Monitor that their staff are following this policy.

6.2.3 Identify, and provide secure access to, equipment that their staff may use to access the Internet.

6.2.4 Managers are required to ensure that a User's personal use of the internet is undertaken within their allocated breaks or out of working hours.

6.3 **All staff must:**

6.3.1 Make themselves aware of this policy and are responsible for adhering to it.

6.3.2 Only access the Internet if they have been authorised to do so.

6.3.3 Not share the access privileges that they have been granted with others.

6.3.4 Not use others' privileges to access the Internet.

7 RAISING AWARENESS / IMPLEMENTATION / TRAINING

7.1 Staff will be made aware of this policy using the trust communication tools, e.g., intranet, Inform, corporate and department induction.

8 MONITORING

8.1 Use of Internet by all users will be monitored to ensure compliance with the trust policy and to ensure and maintain the security of the trust IT networks.

8.2 Where non-compliance with the trust's policy or their Internet access has breached or impacted the security of the trust systems or network, this will be investigated by the trust's Head of Information Governance and brought to the attention of the individual's Line Manager, where appropriate.

8.3 Where the trust has reasonable grounds to believe that a member of staff is breaching this policy, it will monitor staff internet usage.

8.4 When monitoring staff usage of the Internet, monitoring is undertaken in full consideration of Article 8 of the Human Rights Act 1998 and the Information Commissioners Office "The Employment Practice Code: Part 3 Monitoring at Work"

8.5 The consequences of breaching this policy may be considered a serious disciplinary offence and could give rise to a dismissal for gross misconduct.

8.6 Use of trust Internet is subject to UK laws and any abuse will be dealt with appropriately and where appropriate notified to the relevant authorities.

9. REFERENCES

- Computer Misuse Act 1990
- Department of Health (DH)
- Human Rights Act 1998
- Information Commissioners Office (ICO)
- Data Protection Act 2018
- General Data Protection Regulations

10. EQUALITY IMPACT ANALYSIS

This policy has been analysed for impact on equality and does not have an adverse impact on any protected characteristic.