Internet Use Policy

Document Reference	POL047
Document Status	Approved
Version:	V5.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Head of IT		IM&T Security & Resilience Manager
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
3.0	December 2015	Approved at Executive Leadership Board
4.0	December 2017	Approved by ELB
4.1	March 2018	Approved at Information Governance Group
5.0	March 2019	Approved by Management Assurance Group

Document Reference	
Recommended at Date	Information Governance Group 27th March 2018
Approved at Date	Management Assurance Group 20 March 2019
Valid Until Date	March 2021
Equality Analysis	February 2019
Linked procedural documents	N/A
Dissemination requirements	All staff
Part of Trust's publication scheme	Yes

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), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

1. Introduction

This Policy sets out the East of England Ambulance Service NHS Trust (the Trust) position with regard to the use of the internet. This Policy applies to all staff at the Trust including staff who may not be directly employed by the Trust (e.g. agency staff, contractors, self-employed consultants).

1.2 This policy applies to all equipment owned by the Trust which is capable of accessing the internet including, but not limited to, desktop PCs, laptops, tablets and SmartPhones.

1.3 Access to the Internet is provided on all PCs throughout the Trust, by logging onto the Trust's Local Area Network the individual agrees to the terms and conditions of this policy.

1.4 Internet access for non-Trust owned equipment is available on a limited number of sites via the guest wireless. This is strictly for business use only, examples being external companies providing training or giving presentations, meetings with external organisations or members of the public in attendance, or for staff to use personal devices when receiving training so they can access external resources.

2. Purpose and Scope

The purpose of this Policy is to ensure that the internet is used in an appropriate way, and to make staff aware of what the Trust considers to be an acceptable use of this communication medium. This Policy also sets out how the use of the internet is monitored by the Trust.

3. Duties

The Security and Resilience Manager is responsible for ensuring that this Policy is implemented and monitored.

4. Definitions

N/A

5. Internet Use

5.1 The internet is a valuable tool that can support the work of the Trust in a number of ways. The Trust will provide staff (where this is required) with the appropriate and authorised software for accessing the internet. The Trust retains the copyright of any material posted to any forum, newsgroup or web page by any member of staff during the course of their duties.

5.2 The following list of guidelines is not exhaustive and the Trust may add to it from time to time or may treat other actions or conduct as constituting a breach of the spirit of this Policy.

5.3 Internet access needs to be restricted to maintain operational effectiveness and to fulfil our obligations to both national policy and legislation. With numerous IT systems requiring connection to services outside of the Trust bandwidth is critical and must be protected, and where necessary bandwidth for Internet access will be restricted to ensure critical functions are not affected, this includes disconnecting the guest wireless if traffic is such that it interferes with day to day business functions.

5.4 Agreed access levels are listed in Appendices A and B, these are designed to allow staff to access information relevant to their role.

5.5 You may use the internet for work related purposes. You are not permitted to use the internet for personal or private purposes unless such use does not expose the Trust to any expense and does not interfere with the performance of your duties. Such use should take place during your own time (e.g. meal break) and must conform to the guidelines set out in this Policy.

5.6 The use of the internet for personal purposes must be kept brief and be reasonably necessary, whether connected with family, social or other personal needs.

5.7 Staff are not permitted to visit sites containing material of the following nature under any circumstances:

- Games or gaming material.
- Adult material of a sexual or pornographic nature.
- Sites offering gambling services.
- Sites dedicated to any sort of propaganda, which encourages the oppression of a specific group of individuals, for example racist or sexist sites.

5.8 Trade union representatives are entitled to use the internet facilities for legitimate trade union business to communicate with members and full-time union officers. Staff may use the internet to communicate with their trade union officials.

5.9 You must not download, install and/or use any unauthorised or unlicensed software on the Trust's hardware.

5.10 You must not download, install or use any software, routines or files for entertainment purposes such as (but not limited to) video or audio or gaming. Examples of such files are MP3, MPEG, AVI, etc. Anyone in doubt should seek advice from a member of the IM & T Directorate before attempting to download such files.

5.11 You must not use the internet to conduct private or freelance work for the purposes of commercial gain.

5.12 Some materials you find on the internet are copyright works belonging to third parties. You must not print, download or in any way attempt to reproduce or disseminate any document or material from the internet unless you are sure it is not protected by copyright. You must check with a senior member of staff if you are ever in doubt.

5.13 Use of the internet to download, print or in any way reproduce or disseminate any document or material that contains any offensive material or documents, including text, photographs or other images is strictly prohibited. This includes material that is sexually or racially offensive or could in any way offend the principles set out in the Trust's Equal Opportunities Policy and/or Dignity at Work Policy. Any breach of this rule is likely to constitute gross misconduct and result in summary dismissal.

5.14 You must not use internet communications to attempt any unauthorised access to resources (i.e. 'hacking').

5.15 Downloading and/or the viewing of pornography may constitute a criminal offence, and the police will be notified accordingly.

5.16 You should report to your manager any instances where inappropriate sites have been accessed unintentionally (e.g. typographical errors, pop-ups etc).

5.17 All downloaded files will be automatically subject to virus checks, carried out by software that has been installed on all PCs capable of accessing the Internet. It is a disciplinary offence to attempt to disable this software.

5.18 Non-compliance with this policy may be result in disciplinary action being taken.

6. Monitoring of Internet Use

6.1 You should notify your manager or a member of the IM&T Directorate immediately if you suspect that there has been any unauthorised use of the internet by any member of staff.

6.2 The Trust reserves the right to monitor your use of the internet at any time. This may be done by a central web monitoring application or by manual checking of hardware.

6.3 All internet activity is logged automatically on a central web monitoring application. This data can be sorted by user and is archived so historical data can be accessed. All internet activity is logged, including each site and pages within a site that have been accessed. The time and date stamp of the visit and the duration spent on each site and page is also recorded.

Appendix A - Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Internet use	Designated individuals in the Systems and Infrastructure team	Using the web filtering management console	Monthly	Reports generated from the management console	Reports will be sent via line management	Breaches of policy will be reported to line managers of individuals	Breach of policy may lead to disciplinary or legal action being taken.

Appendix B - Equality Impact Assessment

Title: Internet Use Policy

What are the intended outcomes of this work? To ensure that internet access is accessible for all staff that does not impact on operational effectiveness or breach national policy or the law.
Who will be affected? All staff

Evidence
What evidence have you considered?
Disability The policy can be made available in different formats if required.
Gender No evidence found to highlight any differences/ allowances required
Race The policy can be made available in different formats if required.
Age The policy can be made available in different formats if required.

Gender reassignment (including transgender) No evidence found to highlight any differences/ allowances required
Sexual orientation No evidence found to highlight any differences/ allowances required
Religion or belief No evidence found to highlight any differences/ allowances required
Pregnancy and maternity No evidence found to highlight any differences/ allowances required
Carers No evidence found to highlight any differences/ allowances required
Other identified groups No evidence found to highlight any differences/ allowances required

Engagement and involvement *Was this work subject to the requirements for public engagement/consultation?* N/A
How have you engaged stakeholders in gathering evidence or testing the evidence available? N/A
How have you engaged stakeholders in testing the policy/strategy or programme proposals? N/A
For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs: N/A

Summary of Analysis
No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Eliminate discrimination, harassment and victimisation
No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Advance equality of opportunity
No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Promote good relations between groups
No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

What is the overall impact?
No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Addressing the impact on equalities
No actions required

Action planning for improvement

N/A

For the record **Name of person who carried out this assessment:** **Andy Marrs (IM&T Security & Resilience Manager)**
Date assessment completed: **15th December 2017**
Name of responsible Director: **Wayne Bartlett-Syree**
Date assessment was signed: **Approved via email on 20th December 2017**

Appendix C – Eastamb Internet Access Levels

Blocked categories (applies to all staff):

Adult/Sexually Explicit
Advertisements & Pop-Ups
Chat
Criminal Activity
Downloads
Entertainment
Gambling
Games
Hacking
Illegal Drugs
Intimate Apparel & Swimwear
Intolerance & Hate
Peer-to-Peer
Personals and Dating
Phishing & Fraud
Proxies & Translators
Ringtones/Mobile Phone Downloads
Spam URLs
Spyware
Tasteless & Offensive
Unclassified
Violence
Weapons

Blocked categories also includes sites such as Big White Taxi sites, etc which will be categorised in policy as those which are blocked to:

- Ensure that there is protection from external intrusion.
- Ensure that the Trust's image is properly protected.
- Prevent abuse/misuse, which may adversely affect performance, patient and safety care
- Ensure appropriate and effective use

Default Access (All staff)

Alcohol & Tobacco
Arts
Blogs & Forums
Business
Computing & Internet
Education
Fashion & Beauty
Finance & Investment
Food & Dining
Government
Health & Medicine
Hosting Sites
Infrastructure
Job Search & Career Development
Kids Sites
Motor Vehicles
News
Philanthropic & Professional Orgs.
Photo Searches
Politics
Real Estate
Reference
Religion
Search Engines
Sex Education
Shopping
Society & Culture
Sports
Streaming Media
Travel
Web-based Email

Policy Exception – Allows for deviations from policy whereby general access would not normally be permitted for any reason. Examples would be access to specific sites or categories for a particular role or project, either temporarily or permanent.

Technical Access – Specifically for IT support staff. Access is the same as the default level with the addition of sites for remote technical support and downloads, where allowing general access would introduce security vulnerabilities.
Specialist Access – Individuals whose role requires them to access specific sites that fall under the standard blocked category, i.e. Safeguarding.
Communications Access – Specifically for the Communications Team to allow them to monitor various news streaming sites.
Exemptions are in place to all staff for access to the Sky News live stream for operational reasons, also to Youtube, primarily for training and education.

Appendix D – Guest Wireless Internet access levels

Blocked categories:

Adult/Sexually Explicit
Advertisements & Pop-Ups
Alcohol & Tobacco
Arts
Blog & Forums
Chat
Criminal Activity
Downloads
Entertainment
Fashion & Beauty
Finance & Investment
Food & Dining
Gambling
Games
Hacking
Hobbies & Recreation
Hosting Sites
Illegal Drugs
Intimate Apparel & Swimwear
Intolerance & Hate
Kids Sites
Motor Vehicles
Peer-to-Peer
Personals and Dating
Phishing & Fraud
Politics
Proxies & Translators
Real Estate
Religion
Ringtones/Mobile Phone Downloads
Shopping
Spam URLs
Sports
Spyware
Streaming Media (exception in place for YouTube)
Tasteless & Offensive
Travel
Violence
Weapons
Unclassified

Blocked categories also includes sites such as Big White Taxi sites, etc which will be categorised in policy as those which are blocked to:

- Ensure that there is protection from external intrusion.
- Ensure that the Trust's image is properly protected.
- Prevent abuse/misuse, which may adversely affect performance, patient and safety care

- Ensure appropriate and effective use

Permitted Access

Business
Computing & Internet
Education
Government
Health & Medicine
Infrastructure
Job Search & Career Development
News
Philanthropic & Professional Orgs.
Photo Searches
Reference
Search Engines
Sex Education
Society & Culture
Web-based E-mail

Appendix E – EPCR Internet Access

Blocked categories:

Adult/Sexually Explicit
Advertisements & Pop-Ups
Alcohol & Tobacco
Arts
Blogs & Forums
Business
Chat
Criminal Activity
Custom
Downloads
Entertainment
Fashion & Beauty
Finance & Investment
Food & Dining
Gambling
Games
Hacking
Hobbies & Recreation
Hosting Sites
Infrastructure
Intimate Apparel & Swimwear
Intolerance & Hate
Kid's Sites
Motor Vehicles
Peer-to-Peer
Personals and Dating
Philanthropic & Professional Orgs
Phishing & Fraud
Photo Searches
Politics
Proxies & Translators
Real Estate
Religion
Ringtones/Mobile Phone Downloads
Shopping
Society & Culture
Spam URLs
Sports
Spyware
Streaming Media
Tasteless & Offensive
Travel
Violence
Weapons

Permitted Access

Computing & Internet
Education
Government
Health & Medicine
Illegal Drugs
Job Search & Career Development
News
Reference
Search Engines
Sex Education
Uncategorized
Web-based E-mail