NHS
Yorkshire
Ambulance Service
NHS Trust

Internet Policy

Document Author: Head of ICT

Date Approved: February 2018

Document Reference	PO – Internet Policy and Procedure –
Version	V5.1
Responsible Committee	Trust Management Group
Responsible Director	Executive Director of Finance and Performance
Document Author (title)	Head of ICT
Approved by	Trust Management Group
Date Approved	February 2018
Review date	February 2020
Equality impact assessed (yes/no) (full/screening)	Yes
Protective Marking	Not protectively marked

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
1.0	March 2008	David Johnson	A	Initial policy developed.
2.0	March 2011	David Johnson	A	Revisions to format and content.
2.1	Oct 2012	Ola Zahran	D	Existing Internet policy checked for any amendments, formatting changes.
2.2	Feb 2013	Caroline Squires	D	Extensive revisions to existing policy document in relation to content and format.
2.3	March 2013	Caroline Squires	D	Further revisions to content.
2.4	April 2013	Caroline Squires	D	Amendments in response to consultation with Information Governance Working Group Members.
3.0	May 2013	David Johnson	A	Final Approval from SMG May 2013 Full Version Control amendments made.
3.1	Sept 2015	Caroline Squires	D	Significant revisions to format to bring in line with current policy format and minor revisions to content.
4.0	Nov 2015	Ola Zahran Caroline Squires	A	Approved by TMG
5.0	Feb 18	Ola Zahran	D	Approved by TMG – no changes to context. New template.
5.1	Feb 18	Risk Team	D	Document formatted – New visual identity

A = Approved D = Draft

Document Lead = Head of ICT and Information Governance Manager

Associated Documentation:

- Social Media Policy
- Data Protection Policy and Associated Procedures
- Data Protection Policy - Local Care Direct
- Information Governance Policy
- Information Governance Strategy
- ICT Security Policy and Associated Procedure
- Email Policy
- Records Management Policy
- Risk Management Procedures
- Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (NHSD)
- YAS Code of Conduct
- Disciplinary Policy and Procedure
- Bullying and Harassment Policy and Procedure
- Freedom of Information Procedures
- Management of Online and Digital Services Procedure

Staff Summary

Everyone working or acting on behalf of Yorkshire Ambulance Service NHS Trust, including all permanent and temporary staff, contractors, students and researchers have an individual responsibility to make themselves aware of and comply with this policy.
Internet access is provided for business use or for professional development and training, i.e. communicating with business colleagues, researching relevant areas of interest and obtaining appropriate health service and health related information. The Internet can be used for the purpose of research and development.
Limited personal use of Internet facilities is permitted provided that the material accessed is appropriate, is not potentially offensive to others and does not contravene the unacceptable use section of this policy (see section 3.2).
If evidence exists that indicates any user is failing to adhere to this policy or is using the Internet in an inappropriate manner the Trust reserves the right to investigate individual Internet usage under these circumstances.
Unlawful use of the Internet via Trust systems may lead to negative publicity and / or legal liability for the Trust. The Trust will take disciplinary action, which could lead to dismissal, against any employees using the Internet unlawfully

1.0 Introduction

1.1 The internet is a collection of world-wide interconnected computer systems providing access to a variety of information bases known as the World Wide Web (www). It is now firmly established as a major research, information and communication tool within the NHS.

1.2 The Trust endorses the correct and proper use of the Internet, and expects staff to use this facility during the normal course of their work in a professional, ethical and lawful way without compromising the confidentiality, integrity or availability of the Trust's computer network.

1.3 This policy applies to all employees of Yorkshire Ambulance Service NHS Trust (including contractors, bank, agency and temporary staff as well as volunteers) who uses Yorkshire Ambulance Service NHS Trust (YAS) network services and equipment (such as Smartphones and laptop devices) to access the internet.

1.4 **Everyone who is provided with access to the Internet using Trust systems is personally responsible for making themselves aware of and complying with this policy**.

2.0 Purpose/Scope

2.1 The purpose of this policy is to ensure the appropriate use of the Internet, so that all employees are aware of what is deemed as acceptable and unacceptable use of the Internet.

2.2 Compliance with this policy will ensure that access to the Internet will be available and responsive to the business needs of the Trust. This policy will also assist the Trust to comply with NHS security regulations relating to controlled connections to

national computer networks, for example, the Information Governance Assurance Statement for Organisations that use, or plan to use Health and Social Care Information Centre Services (NHSD IG Toolkit).

2.3 Unlawful use of the Internet via Trust systems may lead to negative publicity and / or legal liability for the Trust. The Trust will take disciplinary action, which could lead to dismissal, against any employees using the Internet unlawfully.

3.0 Process

3.1 Acceptable Internet Use

3.1.1 Internet access is provided for business use or for professional development and training, i.e. communicating with business colleagues, researching relevant areas of interest and obtaining appropriate health service and health related information. The Internet can be used for the purpose of research and development.

3.1.2 It is acceptable to download documents from the Internet where this does not contravene any of the unacceptable use activities listed below (see section 3.2).

3.1.3 It is acceptable to access graphics, streaming video or audio files for legitimate work purposes.

3.2 Unacceptable Internet Use

3.2.1 The following list of activities are considered to be unacceptable and may result in disciplinary action being taken, up to and including dismissal:

- Creating, deliberately viewing, downloading or transmitting any offensive, defamatory or otherwise unlawful images, data or other material such as instruction on criminal or terrorist skills, incitement to racial hatred or promotion of cults. Other than instances which demand criminal prosecution the Trust is the final arbiter on what is or is not offensive material or what is or is not permissible access to the Internet.

- Creating, downloading or transmitting pornography.

- Advertising, gambling or soliciting for personal gain or profit.

- Passing indecent, subversive or criminal data across or out of the organisation which may cause harm whether to an individual, groups or the organisation.

- Using the Internet to harass other members of staff by displaying particular websites that they consider offensive or threatening. Users must ensure they are aware of policies which give guidance on acceptable behavior eg Bullying and Harassment Policy and Procedure, and apply these to their use of the Internet.

- Downloading ‘freeware’ or ‘shareware’ software or evaluation software. This is to ensure that software downloaded is not incompatible with existing software and

so that neither you as an individual nor the Trust contravenes licensing laws.

- Intercepting information meant for others or circumventing the access controls of systems and networks of other individuals of the Trust.

- Altering software programs, graphics or other documents without the express permission of the owner.

- Creating, downloading or transmitting data or material in such a way as to violate copyright and intellectual property right laws. Even if downloading is permissible under copyright law, there may be restrictions with regard to copying, forwarding or otherwise distributing files. Software license agreements should be read and adhered to. Staff must not transmit any software or other copyrighted materials from their computer via the Internet.

- Creating or transmitting “junk-mail” or “spam”, including unsolicited commercial webmail, chain letters and advertisements.

- Downloading or streaming video or audio material including MP3 music files for entertainment purposes. Unnecessary or unauthorised Internet use could lead to congestion on the local network and slow down systems for other Trust users.

- Conducting personal transactions in pursuit of personal commercial or business interests or in such a way as to implicate the Trust in those transactions. If in doubt, staff should consult their manager.

3.2.2 Employees should operate the Internet browsers “Back” button immediately should they inadvertently access unsuitable material.

3.2.3 Any member of staff inadvertently accessing material of this nature must report this to the ICT department as their computer and the Trust's firewall will automatically store a copy of the material which must be removed.

3.2.4 However, the Trust notes that access to subjects and sites of a potentially contentious nature may be appropriate in some areas of normal operation and/or in specific circumstances such as approved research. The Trust therefore places special responsibilities of care on staff operating in such areas to ensure that such access is necessary and that other staff are not exposed to any such material without good cause.

3.2.5 Computers and the internet are valuable resources to the Trust and its organisational activities but if used inappropriately may result in severe consequences to both individual users and the Trust. The Trust is particularly at risk with internet access. The nature of the internet makes it impossible to define all inappropriate use. However, all employees are expected to ensure that their use of computers and the internet meets the general requirements of professionalism. The points covered in this section do not represent the totality of possible inappropriate access and use. Users should be aware at all times that the principles of decency

and legality will be applied. A simple rule of thumb could be described as “if the material could cause offence to even one individual then it is probably inappropriate”

3.3 Personal Use

3.3.1 Limited personal use of Internet facilities is permitted provided that the material accessed is appropriate, is not potentially offensive to others and does not contravene the unacceptable use section of this policy (see section 3.2).

3.3.2 The use of the Internet for personal transactions only, such as booking reservations or tickets or the purchase of any goods or services for personal use, is permitted. Employees should regard this facility as a privilege that should be exercised in their own time without detriment to the job and not abused.

3.3.3 The Trust reserves the right to block or limit personal access where the capacity of the network internet connection to cope with business traffic is compromised by personal use.

3.4 Social Media and Networking

3.4.1 Social media is the term commonly used for websites which allow people to interact with each other in some way by sharing information, opinions, knowledge and interests. Examples include Facebook, YouTube and Twitter.

3.4.2 All staff must personally ensure they comply with the Trust’s Social Media Policy, which outlines the Trust’s approach to employee’s personal use of social media and networking and provides practical advice for using it in a responsible manner.

3.4.3 In summary staff:

- Should not reveal confidential information about patients, staff, or the Trust.
- Should not engage in activities on the Internet which might bring the Trust into disrepute.
- Should act in a transparent manner when altering online sources of information such as websites like Wikipedia.
- Should not use the Internet in any way to attack or abuse colleagues.
- Should not post defamatory, derogatory or offensive comments on the Internet about colleagues, patients, their work or the Trust.
- Should discuss any online activities associated with work for the Trust in advance with their line manager and gain approval.
- Should be mindful that displaying an @yas.nhs.uk or nhs.uk e-mail address will link you to the Trust or the NHS.
- Should be aware that anything shared on social networking sites is in the public domain.
- Should not publish pictures, information or comments about the Trust without authorisation.
- Should be mindful that personal views quoted out of context by a third party could bring the Trust into disrepute.

3.4.4 In addition staff must make sure they are familiar with the requirements set out in their employment contract and the Trust Code of Conduct. Staff who are registered with the Health Professions Council should also familiarise themselves with the duties set out in the Standards of Conduct, Performance and Ethics.

3.5 System Monitoring

3.5.1 The Trust has implemented technical measures to actively block access to websites which are deemed "inappropriate" (see Section 3.6). Additionally, all Internet traffic is logged automatically.

3.5.2 Information recorded by these automated monitoring systems can be used to identify an individual user and show, for example, a website or document that a user has been viewing and the time spent browsing. Because of this, staff must not assume privacy in their use of the Trust's Internet system, even when accessing the systems in their personal time i.e. out of paid working hours.

3.5.3 If evidence exists that indicates any user is failing to adhere to this policy or is using the Internet in an inappropriate manner the Trust reserves the right to investigate individual Internet usage under these circumstances.

3.5.4 Managers with concerns should refer to their Human Resources Manager, who will in turn contact the Associate Director of ICT or the Service Delivery Manager in respect of any investigation to be conducted.

3.5.5 Periodic monitoring of internet activity will be undertaken for specific business purposes.

3.5.6 The Trust also reserves the right to carry out detailed inspection of any ICT equipment without notice, where inappropriate activity is suspected.

3.6 Blocking of Inappropriate Content

3.6.1 The Trust will employ software to enable the blocking of sites, the content of which is deemed inappropriate. Attempts to access web sites that display inappropriate content will be logged by the system and may result in disciplinary action being taken against the individual concerned up to and including dismissal without notice.

3.6.2 Deliberate attempts to access certain categories of site, specifically those which display or are connected to child pornography will result in immediate notification to Police. An attempt to access this type of material is a criminal offence. Upon receipt of any information concerning this kind of activity, the relevant Executive Director or nominated deputy should notify the Police immediately and advise the relevant Human Resources Manager. The computer should be left and not used by anyone, allowing this to be seized as evidence for forensic examination by the Police. The details of all persons having access to the computer should be made available to allow a clear evidence trail to be established.

3.6.3 All use of the Internet will be logged by the system monitoring however it is designed

only to identify potential misuse of the organisations systems.

3.6.4 Where a user identifies a site that has been blocked that they require access to as part of their work, they can make a request to have the site opened for use. Requests for a blocked site to be opened for use must be made to the ICT Service Desk with the support of the individuals line manager. By exception the Trust's Information Governance Working Group (membership comprising of all the Trust's Information Asset Owners) may be consulted in relation to decisions to unblock sites, to ensure appropriateness.

3.7 Internet Administration

3.6.5 Only those staff authorised to do so may create or update a site for the Trust on the Internet.

3.6.6 Only Trust ICT staff may load programs or applications (including demonstrations) from the Internet onto the Trust's network or computer systems.

4.0 Training Expectations for Staff

Training is delivered as specified within the Trust Training Needs Analysis (TNA).

5.0 Implementation Plan

5.1 The latest ratified version of this policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this policy and associated procedures during Trust Induction and existing members of staff will be signposted to the policy as part of annual information governance training.

6.0 Monitoring Compliance with this Policy

6.1 All staff (including contractors, temporary, bank, agency staff and volunteers) must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for information governance.

6.2 Failure to follow this policy and related information governance policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member. The Internet access rights of anyone failing to comply with this policy will be revoked with immediate effect.

6.3 In the event of an agency worker or casual worker failing to comply with this policy and related policy and procedure, his / her work with the organisation may be terminated. The contract may also be terminated if the employee is an employee of a contractor.

6.4 A variety of methods will be used for monitoring internet policy compliance including:

- Reporting on Internet Usage
- Reporting on access to illegal or inappropriate web sites as defined in

section 3.2, via ICT system reporting and incident reporting, with review through the Information Governance Working Group.

- Incident reporting on instances of internet virus attacks affecting Trust networks and systems and unlicensed software installation on Trust owned equipment, with review through the Information Governance Working Group.

6.5 Compliance with this policy will be monitored via independent reviews by both Internal and External Audit on a periodic basis.

References

7.1 Legislation

- Great Britain. 1998. *Data Protection Act 1998*. London: HMSO. Available at: www.legislation.gov.uk (Note: this act will be repealed and replaced by the EU General Data Protection Regulations which come into effect on 25 May 2018)
- Great Britain. 2000. *Freedom of Information Act 2000.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2004. *Environmental Information Regulations 2004.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Computer Misuse Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Access to Health Records Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1958 and 1967. *Public Records Act 1958 and 1967.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Crime and Disorder Act 1998*. *Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. *Electronic Communications Act 2000.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2003. The Privacy and Electronic Communications (EC Directive) Regulations 2003. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Human Rights Act 1998*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. *The Regulation of investigatory Powers Act 2000.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1988. *Copyright Designs and Patents Act 1988.* London: HMSO. Available at: www.legislation.gov.uk

7.2 Guidance from Other Organisations

- The Health and Social Care Information Centre. Publications: Information Governance Toolkit. Available at: www.igt.hscic.gov.uk
- Letter from the Chief Executive of the NHS in England, Publications: Department of Health Gateway Reference 9185. Available at: www.connectingforhealth.nhs.uk

8.0 Appendices

Appendix A - Definitions

The definitions or explanation of terms relating to this policy are:-

Defamatory Material	Published (spoken or written) material, which affects the reputation of a person or an organisation and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss.
Harassment	Any unwarranted behavior, which is unreasonable, unwelcome or offensive. This may include physical contact, comments or printed material, which causes the recipient to feel threatened, humiliated or patronised.
Copyright	A term used to describe the rights under law that people have to protect original work they have created.
Pornography	The description or depiction of sexual acts or naked people that are designed to be sexually exciting.
Junk Mail	Unsolicited advertising or promotional material received through the mail or email.

Appendix B - Roles and Responsibilities

All Staff

All staff are responsible for making sure they have read and understood this policy and are aware of the disciplinary and legal action that could potentially be taken if this policy is not followed. Staff should only access the Internet if they have been authorised to do so and are responsible for all actions under their own Network User Account.

Trust Management Group (TMG)

The Trust Management Group consists of Executive Directors and Associate Directors and is chaired by the Chief Executive. The Group carries delegated responsibility from the Trust Executive Group for approving this policy.

Head of ICT

The Head of ICT and Infrastructure, and Voi ce Comms Manager are responsible for ensuring this policy is reviewed periodically and is in line with legislation, Department of Health requirements and best practice. The Document Owner is responsible for overseeing the implementation of this policy including monitoring compliance.

Line Managers

All line managers are responsible for ensuring that all employees are aware of this and related policies.