Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Internet Usage Policy

This procedural document supersedes: the Internet Usage Policy – CORP/ICT 28 v.1

Did you print this document yourself?
The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s)	Chief Information Officer (CIO) and Senior Information Risk Owner (SIRO)
Author/reviewer: (this version)	Roy Underwood – Head of Information Governance & David Linacre – IT Ops Security & Continuity Manager
Date written/revised:	June 2021
Approved by:	Information Governance Committee
Date of approval:	28 June 2021
Date issued:	16 September 2021
Next review date:	Apr 2024
Target audience:	Trust-Wide

Amendment Form

Please record brief details of the changes made alongside the next version number. If the procedural document has been reviewed **without change**, this information will still need to be recorded although the version number will remain the same.

Version	Date Issued	Brief Summary of Changes	Author
Version 2	16 Sept 2021	• Periodic review • Changes to GDPR post Brexit	Roy Underwood/ David Linacre
Version 1	Nov 2017	• This is a new procedural document, please read in full	Roy Underwood/ Joanne Hutchinson

Contents

Page No.

1. INTRODUCTION

The Internet is an important part of the Trust's and the wider NHS communications system. Use of the installed systems/connections are for legitimate work related purposes and are encouraged to improve the quality of work and productivity in patient care, research, operational matters, education and development. However, the Trust must ensure that the increasing use of information technology maintains patient confidentiality, is not misused, and at the same time is secure and accurate. This policy provides guidance on the Trust's expectations for the use of the Internet.

2. PURPOSE

2.1. The Trust's NHS Internet usage policy is designed to help you understand the Trust's expectations for the use of the Internet. All existing policies and procedures apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of Trust resources, harassment, information and data security, and confidentiality.

2.2. Failure to comply with the requirements of this policy, including non-compliance with the Computer Misuse Act 1990, current Data Protection Legislation (the UK General Data Protection Regulation (UK GDPR 2021) and the Data Protection Act 2021), or infringement of copyright, will be regarded as a serious breach of discipline which may result in disciplinary action being taken. Although each case will be judged on its own merits, misuse of the Internet (or any misuse of computer systems) may be considered Gross Misconduct and lead to dismissal.

2.3. Examples of gross misconduct include:

2.3.1. Accessing, downloading and/or distributing pornographic or other offensive material. This may include racial, sexual material or derogatory information about others.

2.3.2. Accessing, downloading and/or distributing information of a discriminatory nature including sexual or racist material or information which is discriminatory towards other groups such as the disabled.

2.3.3. Deliberately or negligently downloading malware (such as viruses, spyware) which expose undermine the Trusts IT security measures and expose Trust computer systems to risk of damage.

2.3.4. Deliberately breaching the Computer Misuse Act 1990 or current Data Protection Legislation, for example, passing patient related data to inappropriate parties.

2.3.5. Downloading, storing and or using copyrighted materials or software such as music and video files, images or computer software.

2.3.6. Administering, supporting or moderating a 3rd party internet site such as discussion groups, fan sites or websites for a business.

3. DUTIES AND RESPONSIBILITIES

The following staff groups will have duties and responsibilities within the Internet Usage Policy.

3.1 Board of Directors

The board of directors is responsible for ensuring that this policy is in place and accessible to staff.

3.2 Information Governance Group

The Information Governance Committee is responsible for:

3.2.1. Ensuring that this policy has been reviewed regularly.

3.2.2. Is up to date and an accurate reflection of the latest laws, regulations and national NHS policies.

3.3 Line Managers

Line Managers are responsible for ensuring that:

3.3.1. Their staff members comply with this policy, associated policies and procedures.

3.3.2. That any suspected breaches of the policy are investigated to ascertain the veracity of such claims or suspicions.

3.3.3. To report any breaches of the policy to the IM&T Department.

3.3.4. Ensuring that any third party users, e.g. external supplier, under their management is aware of this policy and complies with it.

3.4 Doncaster and Bassetlaw Teaching Hospitals (DBTH) Staff Members

3.4.1. All employees are responsible for their own Internet usage in accordance with this policy.

3.4.2. Employees are asked to be vigilant and report any suspected breaches of this policy immediately to their line manager or to HR as appropriate. Although the Trust believes that its approach to implementing the policy is flexible, firm measures are in place to guard against computer misuse. Should a serious breach of this policy be made by a user, then disciplinary action may be taken.

4. PROCEDURE

4.1 Use of the Internet

4.1.1. The internet is a powerful information acquisition and dissemination tool that provides access to unique resources. The Trust reserves the right to restrict access to materials on the Internet where deemed appropriate, this will include access to pornographic and other sites considered offensive. Any restrictions to material by the Trust shall not be deemed to impose any duty on the Trust to regulate the content of material on the Internet. Furthermore, any lack of restriction does not mean that access to that material is authorised.

4.1.2. Use of the internet is made available to employees for work duties, work-related educational purposes and work-related research purposes. Personal use of the internet is limited to lunch breaks and work breaks only – employees may not use the internet for personal use during otherwise working hours. While personal use is permitted during lunch and work breaks, this is only providing that the material accessed is appropriate and not potentially offensive to others. Employees should regard this facility for personal use as a privilege that is only exercised in their own time, without detriment to their job, or the work of others, and not abused. Excessive or inappropriate use of the Internet, including violation of this policy, may result in disciplinary action being taken and/or removal of facilities. It may also lead to termination of employment, or notification to the proper authorities for criminal/civil proceedings depending on the level of violation. The Trust will decide what is considered to be excessive use.

4.1.3. Accessing of pornographic and abusive or offensive material, including sites that may constitute unlawful discrimination on the grounds of race, disability or gender, is not permitted. Such actions may be regarded as gross misconduct and will result in summary dismissal.

4.1.4. The Trust reserves the right to block access to any sites it feels are contrary to Trust policy or incompatible with the ethos of the Trust, including where the amount of data traffic generated adversely affects the Trust's business use of links to the Internet. This may include access to social networking sites and heavy bandwidth sites such as video hosting sites.

4.1.5. It is possible that offensive web sites may be visited by accident or started automatically by an email. If this happens, close down your Internet browser immediately and notify the IT department that an inadvertent access has occurred. Explain why this has occurred and a log will be made. IT Operations will then clean your PC and network profile. You must also advise your line manager or supervisor that an incident of this nature has occurred.

4.1.6. Information obtained through the internet may not be accurate, and the user must check the accuracy, adequacy or completeness of any such information. Furthermore, it is the responsibility of the user when using information obtained from the internet to be aware of copyrighted material in accordance with the permission granted by the publisher.

4.1.7. The threat from viruses and malware and indeed security breaches from the use of the internet are very real. Users must be aware that information and programs downloaded from the internet may contain hidden code capable of destroying data or interfering with the network and data files.

4.1.8. Therefore users must take great care and be vigilant if they are required, as part of their employment, to download or install any executable or program files from the internet; this is an IT Operations task, so please contact the IT Service Desk for advice in this area. Any executable program files not connected with an employee's duties must not be downloaded. All PC's accessing the Internet must have virus-checking software which is installed by the Trust. The use of sophisticated and current anti-malware technologies will protect the Trust from 'attacks' from outside the organisation. Be Cyber aware, be Cyber vigilant.

User Conduct

4.1.9. Confidentiality – You are bound by the Trust's confidentiality and security policies, current Data Protection Legislation, and the Caldicott Principles concerning the information you come across in the course of your work. You may not disclose information relating to any identifiable individual, either patient or staff. Additionally, you may not disclose confidential information relating to any aspect of the Trust's business.

4.1.10. Personal/Patient Identifiable Data – Patient identifiable information or other organisational confidential information must not be transmitted over the Internet unless encrypted with NHS approved software and must only be transmitted over the NHS wide network. Further guidance on the use of Internet based email systems can be found in the Trust's Email Usage policy which should also be read in conjunction with the Trust's IM&T Security policy.

4.1.11. Users should also not undertake the unauthorised transmission to a third party of confidential material concerning the activities of the Trust. All users of the

Trust internet connection who supply their personal details, including credit card details, etc. whilst accessing web sites do so at their own risk. The Trust employs security measures to counteract some types of malware or attempts to extract personal information but cannot guarantee protection against all threats and therefore the onus is on user vigilance.

4.1.12. All users of the Trust internet connection are to respect copyrighted material and utilize copyrighted content in an appropriate way ensuring that it is licensed for Trust use.

4.2 Monitoring Internet Access

4.2.1. Under the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000, the Trust can lawfully monitor employees' Internet activity for the following purposes:

- Gaining routine access to business communications
- Monitoring standards of service and training
- Preventing or investigating crime
- Unauthorised use of systems (Authorised use of Internet is set out under the User responsibilities section of this policy)
- Establishing the existence of facts
- Ascertaining compliance with regulatory standards

4.2.2. The Trust automatically tracks all internet usage and in addition has a system which blocks access to websites it deems inappropriate, or where the use of sites will impact on the business needs of the Trust. This system protects members of staff from accidentally accessing unsuitable websites, and will keep a detailed log of every page visited. The web filter will block access to millions of sites; it cannot block every site deemed inappropriate. The responsibility for accessing inappropriate sites lies ultimately with the user. In addition the system may block sites that are required for legitimate business use. If this happens, users will need to contact the Head of IT Operations (or Head of Information Governance in his absence) by email: dbth.dpo@nhs.net requesting the unblocking of the site in, stating the business need.

4.2.3. If the Trust becomes aware that an employee (or group of employees) may be misusing their internet access in contravention of this policy, steps will be taken immediately to suspend access, and to then consider what the

appropriate level of intervention is going to be, with consideration being given to the options below as follows:

4.2.3.1. Local action by IT in conjunction with Information Governance and P&OD Staff will have the authority to seize any appropriate computer hardware and/or to review individual employee's Internet access if it is considered to be appropriate. Employees will generally be informed of the intended actions after their Network Access has been suspended excepting on advice from Counter Fraud Services or The Police.

4.2.3.2. The Trust Counter Fraud Officer; In accordance with the Trust's counter fraud and corruption plan on any suspicious activity within the scope of this policy, will be refereed to and subsequently investigated by the Trust's Local Counter Fraud Specialist. The results of any such investigation could lead to internal disciplinary and/or civil/criminal prosecution proceedings being instigated against the appropriate person/persons involved.

4.2.3.3. The Police

4.2.4. For Option 1, IT staff will report to the employee's Line Manager and the Head of P&OD only on material found on the computer, which contravenes this and any other relevant Trust policy.

4.2.5. If the Line Manager, in conjunction with Human Resources, considers that this policy has been breached, they will deal with the matter under the Trust's Disciplinary Procedure.

4.2.6. Any information discovered during the Trust's monitoring of internet access will only be used to investigate a breach of this policy and to pursue any subsequent necessary action, and should not be used for any other purpose. The standard process which IT staff will follow when investigating these issues is documented within SoP 13 "Taking Evidence" (in the event of inappropriate use of IT).

5. TRAINING/ SUPPORT

All staff members are required to complete Information Governance Training on an annual basis.

6. MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Internet traffic	Automatically by systems	24/7/365	Alerts are automatically sent to Head of IT Operations
Inappropriate use	Automatically by systems	24/7/365	Alerts are automatically sent to Head of IT Operations

7. DEFINITIONS

Definition	Meaning
IM&T	Information Management & Technology
NHSmail	The email service provided by Accenture in conjunction with NHS Digital on behalf of NHS England
P&OD	People and Organisation Development

8. EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment For All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 1)

9. ASSOCIATED TRUST PROCEDURAL DOCUMENTS

This policy should be read in conjunction with other relevant organisational policies:

- CORP/FIN 1 (D) - Fraud, Bribery and Corruption Policy and Response Plan
- CORP/EMP 2 - Disciplinary Procedure
- CORP/ICT 2 – IM&T Security Policy
- CORP/COMM 24 - Social Media Policy
- CORP/ICT 27– Email and Internal Communications Policy
- CORP/EMP 4 – Fair Treatment for All Policy
- CORP/EMP 27 – Equality Analysis Policy

10. DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website:
https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

11. REFERENCES

The following resources/guidelines have been used in the developments of this policy:

- Current Data Protection Legislation
  - Data Protection Act 2021
  - UK GDPR 2021
- Freedom of Information Act 2000
- Information Commissioners Office
- Records Management: NHS code of practice

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT PART 1 INITIAL SCREENING

Service/Function/Policy/Project/Strategy	Division/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Internet Usage Policy – CORP/ICT 28 v.2	Digital Transformation	Head of IG	New	18/06/2021

1) Who is responsible for this policy? Name of Division/Directorate: Digital Transformation

2) Describe the purpose of the service / ~~function~~ / policy / ~~project/ strategy?~~ Who is it intended to benefit? What are the intended outcomes? Trust Policy

3) Are there any associated objectives? Legislation, targets national expectation, standards: N/A

4) What factors contribute or detract from achieving intended outcomes? – No

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? Details: [see Equality Impact Assessment Guidance] - No

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation] -

6) Is there any scope for new measures which would promote equality? [any actions to be taken] - No

7) Are any of the following groups adversely affected by the policy? No

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	~~Outcome 2~~	~~Outcome 3~~	~~Outcome 4~~

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form – see CORP/EMP 27

Date for next review: Apr 2024

Checked by: Roy Underwood **Date:** 28/06/2021