



**Doncaster and Bassetlaw
Teaching Hospitals**
NHS Foundation Trust

Internet Usage Policy

This procedural document supersedes: the Internet Usage Policy – CORP/ICT 28 v.2



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)	Sam Wilde, Chief Finance Officer
Author/reviewer: (this version)	Roy Underwood – Head of Information Governance Rhona McCleery – Data Security and Protection Manager Tracy Evans-Phillips – Risk Manager
Date written/revised:	October 2026
Approved by:	Information Governance and Cyber Group
Date of approval:	October 2026
Date issued:	October 2026
Next review date:	April 2029 (policy valid until October 2029)
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 3	September 2026	<ul style="list-style-type: none"> • Updated legislative and policy references. • Added Artificial Intelligence (AI) and Generative AI requirements. • Strengthened cyber security and data handling controls. • Added guidance on cloud storage, file sharing and approved digital services. • Updated monitoring, governance arrangements and terminology 	Roy Underwood Tracy Evans-Phillips
Version 2	16 Sept 2021	<ul style="list-style-type: none"> • Periodic review • Changes to GDPR post Brexit 	Roy Underwood/ David Linacre
Version 1	Nov 2017	<ul style="list-style-type: none"> • This is a new procedural document, please read in full 	Roy Underwood/ Joanne Hutchinson

Contents

	Page No.
1 INTRODUCTION	4
2 PURPOSE	4
2.1 Examples That May Constitute Gross Misconduct Include:	4
3 DUTIES AND RESPONSIBILITIES	5
3.1 Board of Directors	5
3.2 Information Governance and Cyber Group	5
3.3 Line Managers	5
3.4 Doncaster and Bassetlaw Teaching Hospitals (DBTH) Colleagues	5
4 PROCEDURE	6
4.1 Use of the Internet	6
4.2 User Conduct	7
4.3 Monitoring Internet Access	8
4.4 Artificial Intelligence and Generative AI	9
5 LEARNING/ SUPPORT	10
6 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT	10
7 DEFINITIONS	11
8 EQUALITY IMPACT ASSESSMENT	11
9 ASSOCIATED TRUST PROCEDURAL DOCUMENTS	11
10 DATA PROTECTION	12
11 REFERENCES	12
APPENDIX 1 - EQUALITY IMPACT ASSESSMENT PART 1 INITIAL SCREENING	13

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.

Internet usage includes access to websites, cloud services, software-as-a-service (SaaS) platforms, collaboration environments, social media, web applications, online storage services and AI-enabled technologies

2 PURPOSE

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.

Non-compliance with the Computer Misuse Act 1990, current Data Protection Legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, or infringement of copyright, as set out in this policy may be investigated under the Trust's Disciplinary Procedure. Depending on the circumstances and seriousness of the matter, conduct may be treated as misconduct or gross misconduct and could result in disciplinary action up to and including dismissal. Each case will be considered on its own facts.

2.1 Examples That May Constitute Gross Misconduct Include:

- Accessing, downloading and/or distributing pornographic or other offensive material. This may include racial, sexual material or derogatory information about others.
- 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.
- Deliberately or negligently downloading malware (such as viruses, spyware) which undermine the Trust's IT security measures and expose Trust computer systems to risk of damage.
- Deliberately breaching the Computer Misuse Act 1990 or current Data Protection Legislation, for example, passing patient related data to inappropriate parties.

- Downloading, storing and or using copyrighted materials or software such as music and video files, images or computer software without appropriate authorisation or licensing.
- Administering, supporting or moderating a third-party website, such as a discussion group, fan site or business website, without authorisation.
- Unauthorised use of public Artificial Intelligence systems or internet-based services resulting in the disclosure of confidential, patient, staff or commercially sensitive information.

3 DUTIES AND RESPONSIBILITIES

The following colleague 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 colleagues.

3.2 Information Governance and Cyber Group

The Information Governance and Cyber Group is responsible for:

- Ensuring that this policy has been reviewed regularly.
- Ensuring that it remains up to date and accurately reflects applicable legislation, regulation and national NHS policy.

3.3 Line Managers

Line Managers are responsible for ensuring that:

- Their colleagues comply with this policy, associated policies and procedures.
- That any suspected breaches of the policy are investigated to ascertain the veracity of such claims or suspicions.
- To report any breaches of the policy to the Digital Department.
- 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) Colleagues

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

Colleagues must remain vigilant and report any suspected breach promptly to their line manager, the Digital Department or People and Organisational Development, as appropriate. Suspected breaches may be investigated and, where proven, may result in action under the Trust's Disciplinary Procedure.

4 PROCEDURE

4.1 Use of the Internet

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.

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.

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 unless access is for a legitimate Trust purpose. Such conduct may be investigated under the Trust's Disciplinary Procedure and, depending on the circumstances, may constitute gross misconduct and result in disciplinary action up to and including dismissal.

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.

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.

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.

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.

Users must take appropriate care when downloading files from the internet. Software, executable files and browser extensions must not be downloaded or installed unless authorised through the Trust's approved Digital Services processes. Trust-managed devices must use the security controls provided by the Trust, and users remain responsible for exercising appropriate caution. Be Cyber aware, be Cyber vigilant.

Users must remain alert to cyber security threats including phishing emails, malicious websites, fraudulent QR codes, social engineering attempts and other methods designed to gain unauthorised access to Trust systems or information.

Any suspected cyber security incident must be reported immediately through the Trust's established reporting processes and the IT Service Desk.

4.2 User Conduct

Confidentiality – You must comply with the Trust's confidentiality and security policies, current data protection legislation and the Caldicott Principles in relation to information accessed or obtained in the course of your work. Information relating to an identifiable patient, colleague or other individual must not be disclosed without appropriate authority. Confidential information relating to any aspect of the Trust's business must also be protected.

Personal/Patient Identifiable Data – Personal, confidential or commercially sensitive information must only be transmitted using Trust-approved systems and secure methods appropriate to the sensitivity of the information and the intended recipient. 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 Information Management & Technology Security policy.

Patient-identifiable, staff-identifiable, commercially sensitive or other Trust information must only be stored, shared, processed or transmitted using Trust-approved systems, applications and storage locations. Colleagues must ensure that information is handled in accordance with current data protection legislation, Trust Information Governance requirements and associated policies.

Public cloud storage services, file-sharing platforms and other internet-based services must not be used for the storage, sharing or processing of Trust information unless they have been formally approved through Trust governance processes.

Colleagues must not upload Trust information, including patient-identifiable, staff-identifiable, commercially sensitive or confidential information, to publicly available Artificial Intelligence (AI) platforms. The use of AI technologies must comply with the Trust Artificial Intelligence Policy (CORP/ICT 32).

Users must not transmit confidential Trust material to a third party without appropriate authority. Users who provide personal or payment details while accessing websites do so at their own risk. Although the Trust applies security measures to reduce cyber threats, it cannot guarantee protection against every threat; users remain responsible for exercising appropriate caution.

All users of the Trust internet connection are to respect copyrighted material and utilise copyrighted content in an appropriate way ensuring that it is appropriately licensed or otherwise permitted for Trust use.

4.3 Monitoring Internet Access

Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Trust may monitor use of its systems and internet services where this is lawful, necessary and proportionate. Monitoring will be undertaken for specified purposes and in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018, relevant privacy information and Trust governance arrangements, including:

- 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

Monitoring may include web access logs, cloud service usage, AI platform access logs, security event monitoring, network traffic monitoring and other lawful cyber security monitoring activities undertaken to protect Trust systems and information assets.

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 colleagues 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 log a ticket with the IT Helpdesk who will pass to the Operation Team for resolution.

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:

Local action by the Digital Team in conjunction with Information Governance and People and Organisational Development Department colleagues 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.

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 referred 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.

For Option 1, IT colleagues 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.

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.

Any information obtained through monitoring will be used only for lawful, specified and proportionate purposes, including protecting Trust systems and information, maintaining service availability, investigating suspected misuse, preventing or detecting crime and demonstrating compliance with legal or regulatory requirements. Monitoring information must not be used for any incompatible purpose.

4.4 Artificial Intelligence and Generative AI

The Trust recognises the emerging role of Artificial Intelligence (AI) technologies in supporting administrative, analytical and operational activities.

Colleagues must comply with the Trust Artificial Intelligence Policy (CORP/ICT 32) when using any AI-enabled technology.

Microsoft Copilot may be used for NHS business where its use is permitted by NHS England and complies with the Trust Artificial Intelligence Policy (CORP/ICT 32) and associated Trust guidance. This includes the free version of Microsoft Copilot; however, patient-identifiable information, staff-identifiable information, commercially sensitive information or any other confidential Trust information must not be entered, uploaded or shared.

Only AI services permitted by NHS England or formally approved by the Trust may be used for Trust business. Approval may be limited to specific products, versions, licences, accounts, purposes or information classifications. Colleagues must not assume that an AI service is approved solely because it is supplied by Microsoft, described as Copilot or publicly available. Other public AI services, including ChatGPT, Claude, Gemini, Perplexity, DeepSeek or similar tools, must not be used for Trust business unless formally approved.

AI-generated output must be reviewed by an appropriately competent person for accuracy, completeness, bias, confidentiality, intellectual property and suitability for the intended purpose before it is used to support decisions, reports, communications or operational activities. Accountability remains with the colleague using the output and the Trust. Proposed uses of AI may require additional information governance, data protection, procurement, clinical safety or digital assurance before implementation.

5 LEARNING/ SUPPORT

Learning requirements for colleagues will be determined by their role and the competencies required to work safely and effectively. These requirements include national, local and role-specific mandatory learning and are set in line with Trust and professional standards.

Role-specific learning will be defined by the relevant subject matter expert or topic lead and coordinated through the Trust's agreed governance arrangements.

All mandatory and role-specific learning requirements, completion status and competency records will be held in the colleague's personal Electronic Staff Record (ESR).

For further guidance, please see: **CORP/EMP 66 – Mandatory Learning Policy and DBTH Mandatory Learning Framework**

All colleagues 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
AI	Artificial Intelligence
Digital Team	Trust Digital Services Department
NHSmail	NHS national email service

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), the Equality Diversity and Inclusion Policy (CORP/EMP 59) and the Civility, Respect and Resolution Policy (CORP/EMP 58).

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/COMM 24 - Social Media Policy
 CORP/COM 31 – Communications and Media Policy
 CORP/EMP 2 - Disciplinary Procedure
 CORP/EMP 27 – Equality Analysis Policy
 CORP/EMP 59 – Equality, Diversity and Inclusion Policy
 CORP/FIN 1 (D) - Fraud, Bribery and Corruption Policy and Response Plan
 CORP/ICT 02 – Information Management & Technology (IM&T) Security Policy
 CORP/ICT 07 – Data Protection Policy
 CORP/ICT 09 – Information Governance Policy
 CORP/ICT 21 – Information Risk Management Policy
 CORP/ICT 27– Email and Internal Communications Policy
 CORP/ICT 29 – Acceptable Use Policy – IT Systems
 CORP/ICT 32 – Artificial Intelligence 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).

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 2018 [Data Protection Act 2018](#)

UK General Data Protection Regulation (UK GDPR) [Data protection: The UK's data protection legislation - GOV.UK](#)

Freedom of Information Act 2000 [Freedom of Information Act 2000](#)

Information Commissioner's Office: [Information Commissioners Office](#)

NHS Digital Acceptable Use guidance [Acceptable use policy: NHS Notify - NHS England Digital](#)

NHS England Cyber Security guidance [NHS England » Cyber Security](#)

NHS Records Management Code of Practice [records management code of practice - nhs england digital](#)

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.3	Digital Transformation	Roy Underwood	Existing	October 2026
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: April 2029 (policy valid until October 2029)				
Checked by: Rhona McCleery		Date: October 2026		