Policy:

IMST 004 - Data & Information Acceptable Use

Executive Director Lead	Executive Director of Finance & SIRO
Policy Owner	Assistant Deputy Director of IMS&T (Informatics and Architecture)
Policy Author	Data Protection Officer

Document Type	Policy
Document Version Number	Version 1.3
Date of Approval By PGG	28/11/2022
Date of Ratification	January 2023
Ratified By	ARC
Date of Issue	November 2022
Date for Review	30/11/2025

Summary of policy

This policy provides guidance on the use of data, information and associated systems within the Trust.

Target audience	SHSC staff and people authorised to access the SHSC network

Keywords	Internet, acceptable use, social media

Storage & Version Control

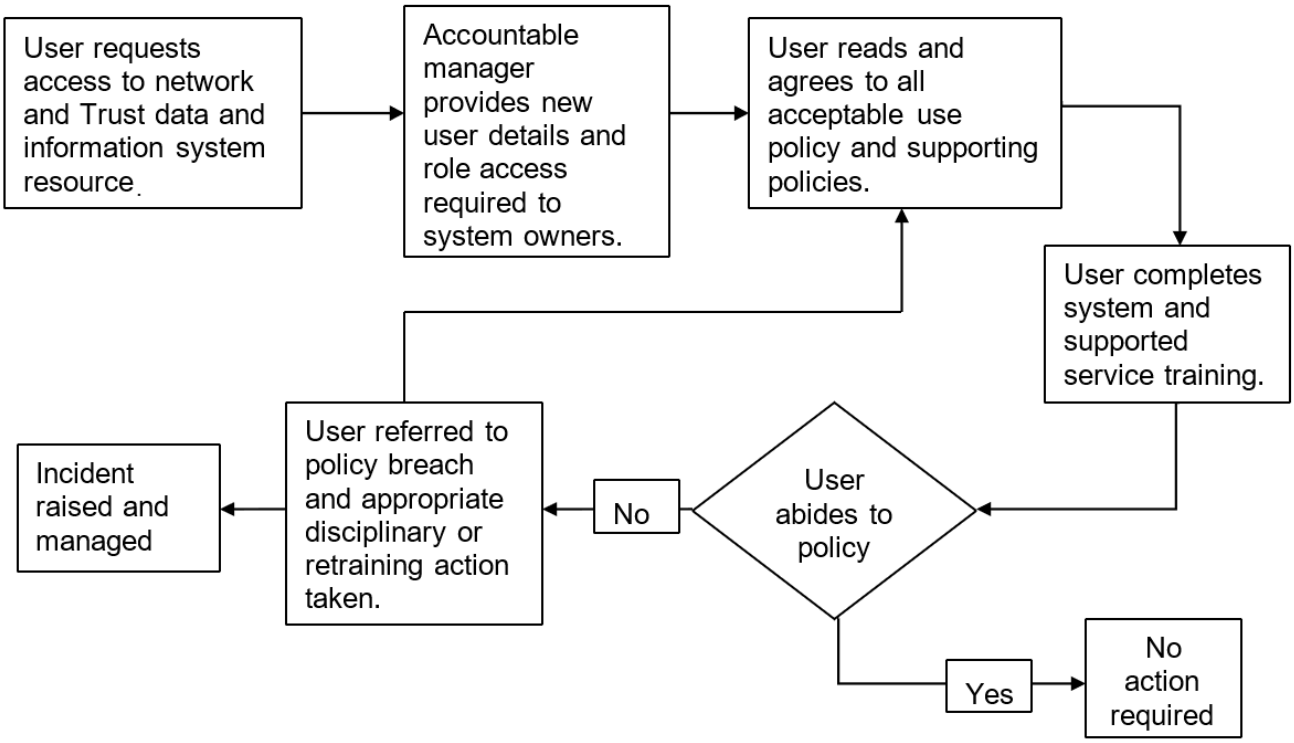
Version 1.3 of this policy is stored and available through the SHSC intranet/internet.. This version of the policy supersedes the previous version (V1.2 11/2019). Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

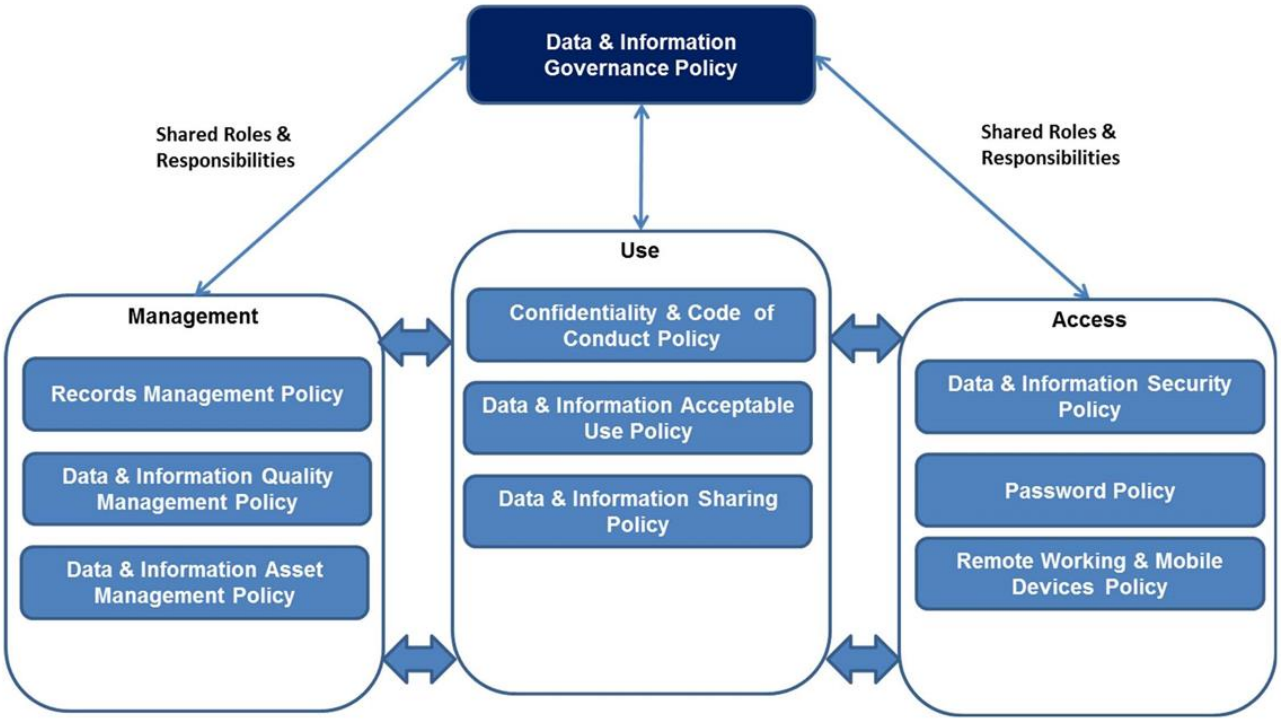
Version No.	Type of Change	Date	Description of change(s)
1	Policy created	03/2018	New policy to replace the previous Internet Acceptable Use Policy as part of a comprehensive review of information governance policies.
1.1	Revision	10/2019	Updates for legislative and monitoring changes and contact details. Clarification on e-mail use.
1.3	Revision	08/2022	Removal of prohibition of Cloud storage, updates for staff and organisational change.

Contents

Flowchart



The Data & Information Governance Policy provides the overarching shared roles and responsibilities needed to satisfy complete trust Data, Information and System ownership and management.



1 Introduction

This policy sets out the expectations of the Trust for individual's appropriate use of the Internet and systems, when accessed using Trust clinical & business solutions and equipment.

This policy governs all IT acceptable use and behaviour, if conflict exists in other policies and this Policy, the Data & Information Acceptable Use Policy takes precedence.

2 Scope

The scope of this document is to outline the Trust's policy for Acceptable Use for all data, information, system management and protection.

This policy applies to all staff and services within the Sheffield Health & Social Care (SHSC), including private contractors, volunteers and temporary staff and to those organisations where we provide commissioned services.

Shared governance and compliance areas for data and information include:

- NHS Digital & England Guidance
- Data Security & Protection Toolkit
- Cyber-Security Best Practices
- Information Technology Service Management
- General Data Protection Regulation
- Caldicott Principles
- Data & Information Quality Management
- ISO27001 Information Security Management Systems

The policy supports the Trusts' need to continually improve, protect and manage all digital, data and information assets according to legislation and best practice through a collaborative approach.

Systems

All manual and electronic information systems owned, operated or managed by the Trust, including networks and application systems, whether or not such systems are installed or used on Trust premises.

Other systems brought onto Trust premises including, but not limited to, those of contractors and third-party suppliers, which are used for Trust business.

Users

All users of Trust information and/or systems including Trust employees and non-Trust employees who have been authorised to access and use such information and/or systems.

Data & Information

All information collected or accessed in relation to any Trust activity whether by Trust employees or individuals and organisations under a contractual relationship with the Trust.

All information stored on facilities owned or managed by the Trust or on behalf of the Trust.

All such data & information belongs to the Trust unless proven otherwise.

3 Purpose

The purpose of this policy is to regulate access to and the use of the Internet and related systems by means of Trust equipment.

4 Definitions

Social Media

Social media is a generic term which refers to websites, online tools and other interactive communication technologies which allow users to interact with each other by sharing information, files, opinions, knowledge and interests. Social media involves the building of communities or networks, thereby encouraging participation and engagement. Examples of social media include Facebook, Twitter, LinkedIn, SnapChat and Tumblr, as well as YouTube, Flickr, Instagram, TikTok and other image and video-sharing sites.

Cloud Storage

Cloud Storage refers to third party online storage services such as Google Drive, Dropbox and OneDrive. Files stored on these services can usually be accessed via any web browser and often have the capability to be synchronised to multiple computers and mobile devices such as mobile phones and tablets. They may also have the facilities for sharing files with other internal and external parties.

5 Detail of the policy (title needs to be changed as appropriate)

This policy provides guidance on the use of data, information and associated systems within the Trust, and includes arrangements for use of the Guest WiFi.

6 Duties

The strategy combines traditional Information Asset (IAO / IAA), data governance, data quality and (ITSM) system management roles and responsibilities into a single accountable shared Business Information Management framework.

Role		Responsibility	Description
Chief Information Officer	CIO	Chief Digital Information Officer	Responsible for the Information Technology that supports the overarching strategies of the Trust.
Chief Clinical Information Officer	CCIO	CCIO	Providing a vital voice for clinical strategy, allowing new IT, Data & Information products to help improve the provision of healthcare.
Senior Information Risk Owner	SIRO	Director Finance	Owns the Trusts information risk policy and risk assessment process.
Caldicott Guardian	CG	Director Medical	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.
Data Protection Officer	DPO	DPO	Supporting Trust - wide Data & Information governance in accordance with UK GDPR, NHS Digital & England and Data Security and Protection Toolkit

Cyber Security Officer	CSO	Assistant Deputy Directors IMST	Supporting the Trust to continuously assess, implement and manage Trust-wide cyber-security, and removing identified vulnerabilities with support from all technical and business managers and users.
Information Asset Owners	IAO	Directorate	Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems.
Information Asset Managers	IAM	System/Service Managers	Primary administrative and management responsibilities for segments of data primarily associated with their functional area

Each Data and Information role has clear responsibilities for data, information and system management within their respective service domains and role accountability, supported by natural hierarchy escalation and incident management.

All staff who use Trust information systems (including manual systems as well as electronic ones) plus other authorised users of systems are required to adhere to this policy.

7 Procedure

7.1 Adherence to this policy

Users requiring access to the Trust network and the Internet via Trust facilities will be presented with a statement on logging on to the network which reminds them that unauthorised use of Trust systems is not permitted, that use of systems may be monitored and audited, that they have responsibilities under law and Trust policy and that misuse of systems may lead to disciplinary or legal action, and they will be required to accept the statement before proceeding.

Where users are granted individual access to the Trust network and the Internet via an individual user account they must not allow other people, including colleagues, service users, carers or members of the public, to access the network or the Internet via that account by sharing their logon details or allowing use of the account once it has been logged on. The named user is responsible for all access and actions made on that account.

Failure to comply with this policy and procedures may have serious consequences for the individual including civil, criminal and/or disciplinary proceedings.

7.2 Access to and use of electronic systems

The Trust provides access to electronic systems to employees and authorised non-Trust employees only for use in their:

- Work duties
- Work related educational purposes
- Work related research purposes

The Trust allows limited personal use of the internet in the user's own time and only where it does not interfere with their work duties or the work of others.

Where internet use by a particular member of staff is deemed to be excessive, the IT Department will notify the appropriate line manager for further investigation. Managers may also request detailed internet usage reports from the IT Department.

The Trust reserves the right to prevent access to any internet sites it considers inappropriate or detrimental to Trust business.

7.3 Ensuring integrity of the system

The Trust monitors use of the internet in line with legislation, guidance and Trust policy.

The Trust reserves the right to remove or amend access to the internet at any time in order to protect and preserve the integrity and security of Trust systems.

7.4 Monitoring

All internet activity on Trust systems is logged automatically.

Monitoring logs are audited periodically.

Any monitoring will be carried out in accordance with legislation such as the Regulation of Investigatory Powers Act 2000, Data Protection legislation, the Human Rights Act 1998 and Trust policy regarding monitoring and privacy.

Where staff used of the internet is suspected to be inappropriate or excessive, the appropriate manager may request detailed internet usage reports for their staff and monitoring information may be used in support of disciplinary action.

Where appropriate a user's account will be suspended. This suspension will only be cleared once the user has successfully completed the appropriate online Information Governance e-learning module.

7.5 User Rights and Responsibilities

When accessing the Internet, users must:

- Comply with Trust policies including this policy, the Equal Opportunities and Dignity at Work Policy and the Unacceptable Behaviour Policy when using the Internet for both work and personal use.

- Log out of the Internet when not at the computer for a period of time or when it is not being actively used – logging software measures the total time of connection even when the user is not interacting with the webpage displayed because the connection is still using network capacity.

When accessing the Internet, users must not:

- Use the Internet for any purpose that conflicts with any Trust Policy, Code of Conduct or their Contract of Employment.

- Use the Internet to conduct private or freelance work for the purpose of commercial gain including gambling.

- Use the Internet to create, hold, transmit or view material that has an obscene, pornographic or sexually offensive content (other than for properly authorised and lawful healthcare work or research).

- Use the Internet to create, hold, transmit or view material that has an offensive (for example, racist, sexist, homophobic), defamatory, harassing or otherwise illegal content or information relating to terrorism.

- Use the Internet to undertake or access information about hacking (the IT department will co-ordinate any activities in relation to “ethical-hacking” in order to test the security of Trust systems).

- Use the Internet to make untrue, inaccurate, misleading or offensive statements about any person or organisation.

- Download or install any unauthorised software on Trust equipment without prior authorisation from the IT department.

- Use Internet-based file sharing applications, unless explicitly approved and provided as a service by the Trust.

- Upload or download private data (e.g. private pictures) to and from the Internet.

- Download copyrighted material such as software, text, images, music and video from the Internet without the appropriate license of permission.

- Use external, web-based e-mail services (e.g.hotmail.com) or other messaging applications (such as WhatsApp) for business communications and purposes.

- Use the Internet to participate in online games or subscribe to active web channels that broadcast frequent updates to PCs such as news feeds or streaming video or audio unless specifically approved by the SHSC IT Department.

- Store e-mail or other personal details together with the password or account details on external websites.

Information found on the Internet is subject to minimal regulation and as such must be treated as being of questionable quality. Users should not base any business-critical decisions on information from the Internet that has not been independently verified.

Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not been given explicit access or authorisation.

Where a user has a valid work need to access a site which has been blocked they may request it to be unblocked by submitting an electronic request form approved by their manager.

Only Trust approved, standard and supported software for web and telephony conferencing and collaborative working may be used.

Trust equipment may be connected to home Internet connections or free public connections in order to log in to the Trust network via the approved Trust software. Trust equipment should not be connected to other (non-work) Internet connections for non-work purposes.

7.6 Inadvertent misuse of the Internet

A user who inadvertently accesses a site which contains material that is unacceptable and inappropriate, as specified above, must disconnect from it immediately and inform the IT Service Desk.

7.7 Use of the Guest Wi-Fi

SHSC provides separate guest Wi-Fi at some of its sites. Anyone using the guest WiFi is responsible for any Internet access and actions taken whilst they are connected to the SHSC guest Wi-Fi in accordance with the terms and conditions set out in Appendix C.

The Trust will block access to inappropriate sites via the guest Wi-Fi but does not accept responsibility for any content that users may be able to access. The guest WiFi must not be used to access inappropriate material even if it is not blocked automatically.

The Trust reserves the right to refuse, suspend or terminate access to the guest Wi-Fi without notice.

7.8 Access via Govroam

Govroam allows staff to connect to the Internet whilst visiting other public sector sites. When using Govroam, staff must abide by the policies of their employing or host organisation in relation to acceptable use of the Internet.

7.9 Social Media (Blogging and Social Networking)

The use of social media has expanded rapidly for work purposes as well as for personal and social purposes and whilst it can have benefits it also presents risks to the individual and the Trust, particularly due to its widespread use outside of work and the fact that social computing can blur the boundary between work and personal life. As an informal method of communication it is easy to publish content that you may later regret and which may not be appropriate in a work context. Such information may end up having a much wider audience than anticipated and cannot later be retracted.

Official Trust social media accounts are operated by the SHSC Communications Department. Other members of staff or teams are not permitted to operate open social media accounts for Trust purposes unless authorised by the Communications Manager.

Staff should take care to use social media in a manner that is consistent with the terms and conditions of their employment or association with the Trust. For example, individuals should not post content that breaches confidentiality, contains inappropriate comments about colleagues or service users, is abusive or hateful, or would potentially cause embarrassment or be detrimental to the reputation of the Trust. In addition, where appropriate, individuals should identify that any views expressed are their own and not those of their employer.

When posting on social media users must be careful not to infringe copyright. They should avoid disclosing information which on its own or in combination with other information available elsewhere could be used for identity theft, or to breach security controls on other systems (for instance giving out their mother's maiden name or the user's home address or date of birth).

The Trust may monitor the use of social media for inappropriate use by staff and may investigate any reported misuse which may lead to disciplinary action.

Where access to social media is allowed via the Trust network, users must not make excessive use of it, and must not use it where such use would adversely affect the performance of the Trust's networks or systems, or interfere with their own work or that of others.

Users may not access social media for non-work purposes on their own equipment during work time.

Failure to adhere to such guidance may result in the individual being subject to disciplinary procedures.

See the "Social Media Policy" available via the SHSC intranet.

7.10 Email

E-mail is a communication tool, not a record management system. Where e-mails contain information which is needed as part of the care record or as part of a corporate record the recipient should transfer the information to the appropriate record management system where it will be available to other authorised users when needed and will be retained for the appropriate period of time.

Users shall not use the Trust's e-mail to conduct private or freelance work for the purpose of commercial gain.

Users shall not create, hold, send or forward e-mails that have obscene, pornographic, sexually or racially offensive, defamatory, harassing or otherwise illegal content (if you receive such a message you should report it to the IT Service Desk immediately).

Users shall not create, hold, send or forward e-mails that contain statements that are untrue, inaccurate, misleading or offensive about any person or organisation.

Users shall not access and use another user's e-mail account without permission. If it is necessary to access another user's account then contact the IT Service Desk for details of the relevant procedure. Users should be aware that access to their email account by authorised individuals may be necessary in periods of absence for business continuity reasons.

Users shall not send e-mail messages from another member of staff's e-mail account or under a name other than their own. (Secretaries/PAs may send e-mails in their own name on behalf of their manager if instructed to do so).

Users shall not use e-mail for political lobbying.

Users shall not knowingly introduce to the system, or send an e-mail or attachment, containing malicious software, for example, viruses.

Users shall not forge or attempt to forge e-mail messages, for example, "spoofing".

Users shall not send or forward chain letters or other similar non-work related correspondence.

Users shall not send unsolicited e-mails (spam) to large numbers of users unless it is directly relevant to the recipient's work. (Use staff bulletin/notice boards where appropriate).

Users must not automatically forward mail from their Trust e-mail account or send confidential or sensitive Trust information to their own non-NHS e-mail accounts. Examples of non-NHS e-mail accounts include Hotmail, G-mail and e-mail services provided by internet service providers.

The personal use of e-mail is permitted as long as messages are sent in the user's own time, they do not detract from the user's work duties and they do not disrupt the work of others. Personal e-mails should be stored in a folder marked "personal" and e-mails should be marked as "personal" in the subject header.

7.11 Cloud Storage

Cloud storage of confidential Trust data or hosting of Trusts systems will only be permitted once it has been subject to evaluation as part of a Data Processing Impact Assessment (DPIA). Compilation of a DPIA will serve to identify any risks introduced by new processing and will identify to what extent the risks can be addressed. The DPIA must be approved by the SIRO and Caldicott Guardian before the processing can commence.

7.12 Reporting Information Incidents and Weaknesses

An Information Incident is an event that could compromise the confidentiality of information (for example if it is lost or could be viewed by or given to unauthorised persons), the integrity of the data (if it could be inaccurate or the content could have been changed) or the availability of the information (access).

Examples of information incidents are:

- Potential and suspected disclosure of NHS information to unauthorised individuals.
- Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored.
- Disruption to systems and business processes.
- Attempts to gain unauthorised access to computer systems, e.g. hacking.
- Records altered or deleted without authorisation by the data "owner".
- Virus or other malicious malware attacks (suspected or actual).
- "Blagging" offence where information is obtained by deception.
- Breaches of physical security e.g. forcing doors or windows to access secure rooms or filing cabinets containing NHS sensitive or other UK Government information left unlocked in an accessible area.
- Leaving a desktop or laptop unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Human error such as emailing data by mistake.
- Covert or unauthorised recording of meetings and presentations.
- Damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges.
- Deliberate leaking of information.
- Insider fraud.[1]
- Smartcard or application misuse.
- Smartcard theft.

[1] Where any incidents involving suspected fraud are identified, the Trust's Counter Fraud, Bribery and Corruption Policy should be followed and advice sought from the Local Counter Fraud Specialist (christaylor2@nhs.net)

- Non-compliance of local or national RA policy.
- Any unauthorised access of NHS applications.
- Any unauthorised alteration of patient data.

The Trust handles considerable amounts of patient data, much of which is sensitive. An information incident involving sensitive data, especially patient confidential information, is considered to be a data/information breach and must be reported.

All information management and technology incidents and weaknesses must be reported via Trust incident reporting procedures (see Trust Incident Management Policy and Procedure).

Incidents that present an immediate risk to the Trust should be escalated through local supervisor & manager, IT Service Desk & Data Protection Officer.

SIRO & Data & Information Governance Group Reporting (DIGG)
The Data Protection Officer will keep SIRO & DIGG informed of the information security status of the Trust by means of regular reports and immediate alerts where an immediate risk is identified.

8 Development, Consultation and Approval

The Internet Acceptable Use policy was originally developed by the city-wide Information Governance Group (SCT and PCTs).

It was tabled at the SCT Information Governance Committee.

It was sent, along with other IG policies to JCF in June 2007 (in light of the heavy workload due to the Foundation Trust application, the policies were considered outside the meeting by staff side).

Following consultation with staff side, the policies were agreed by the Information Governance Committee in September 2007.

The policies were re-formatted in line with revised Trust requirements.

The policies in new format were approved by the Information Governance Committee on 10 March 2008.

The policies were approved by the Performance Information Group on 18 March 2008.

This policy was revised and submitted to the Information Governance Steering Group in October 2010.

Further amendments made following submission to the Information Governance Steering Group, then submitted to the Performance Information Group.

The policy was reviewed and minor amendments made in February 2013.

The policy was reviewed and minor amendments made in February 2014.

The policy was expanded to become a wider Acceptable Use policy in line with NHS Digital best practice and Internal Audit recommendations in February 2018.

This policy was revised in October 2019 to update references and contact details and to clarify the use of e-mail details for submission to the November 2019 Data & Information Governance Board.

The policy was revised in August 2022 following discussion within IMST for submission to the September 2022 Data & Information Governance Group.

9 Audit, Monitoring and Review

This section should describe how the implementation and impact of the policy will be monitored and audited. It should include timescales and frequency of audits.

If the policy is required to meet a particular standard, it must say how and when compliance with the standard will be audited.

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
Compliance with this policy in terms of use of the Internet and related systems	Review in light of any incidents, staff requests and suggestions	Information Governance Manager; Assistant Deputy Directors IMST; Data Protection Offcier; IT Dept.	Annual	Data & Information Governance Group	Information Governance Manager; Assistant Deputy Directors IMST	Data & Information Governance Group

Policy documents should be reviewed every three years or earlier where legislation dictates or practices change. The policy review date should be written here – 11/2025

10 Implementation Plan

Action / Task	Responsible Person	Deadline	Progress update
Upload new policy onto intranet and remove old version	Communications Dept.		
Notify adoption of new policy via Trust Connect newsletter	Communications Dept.		

11 Dissemination, Storage and Archiving (Control)

This section should describe how the new policy will be disseminated. It says where the policy will be made available and to whom. This will normally be that the policy is available on the Trust's intranet and available to all staff.

It makes it plain that any previous versions must be deleted and describes the archiving and storage arrangements for the current and previous versions of the policy.

It says who is responsible for archiving and version control, and what they should do.

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1.0	08/2018	08/2018		
1.2	11/2019	11/2019		
1.3	November 2022	November 2022	November 2022	N/A

12 Training and Other Resource Implications

Departmental managers are responsible for ensuring that their staff are aware of and comply with this policy.

Staff and other people who are given access to the Trust network will be made aware of their responsibilities at time of issue.

13 Links to Other Policies, Standards (Associated Documents)

- Social Media Policy for Staff
- Copyright, Designs and Patents Act 1998
- Counter Fraud, Bribery and Corruption Policy

14 Contact Details

Title	***Name***	***Phone***	***Email***
Senior Information Risk Owner (SIRO)	Phillip Easthope	0114 3050765	Phillip.easthope@shsc.nhs.uk
Assistant Deputy Director of IMS&T	Ben Sewell	0114 2711144	Ben.sewell@shsc.nhs.uk
Information Governance Manager	Katie Hunter	0114 2716723	katie.hunter@shsc.nhs.uk
Data Protection Officer	John Wolstenholme	0114 3050749	John.wolstenholme@shsc.nhs.uk

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement. **I confirm that this policy does not impact on staff, patients or the public.**	***I confirm that this policy does not impact on staff, patients or the public.*** Name/Date: J Wolstenholme, 18 Nov 2022	**YES,** Go to **Stage 2**

Stage 2 Policy Screening and Drafting Policy - Public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

Stage 3 – **Policy Revision** - Make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section

SCREENING RECORD	Does any aspect of this policy or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
Age			
Disability			
Gender Reassignment			
Pregnancy and Maternity			

Race			
Religion or Belief			
Sex			
Sexual Orientation			
Marriage or Civil Partnership			

Please delete as appropriate: - Policy Amended / Action Identified (see Implementation Plan) / no changes made.

Impact Assessment Completed by:
Name /Date

Appendix B

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	✓
2.	Is the local Policy Champion member sighted on the development/review of the policy?	✓
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	N/A
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	✓
5.	Has the policy been discussed and agreed by the local governance groups?	✓
6.	Have any relevant recommendations from Internal Audit or other relevant bodies been taken into account in preparing the policy?	✓
	Template Compliance	
7.	Has the version control/storage section been updated?	✓
8.	Is the policy title clear and unambiguous?	✓
9.	Is the policy in Arial font 12?	✓
10.	Have page numbers been inserted?	✓
11.	Has the policy been quality checked for spelling errors, links, accuracy?	✓
	Policy Content	
12.	Is the purpose of the policy clear?	✓
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	✓
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	✓
15.	Where appropriate, does the policy contain a list of definitions of terms used?	✓
16.	Does the policy include any references to other associated policies and key documents?	✓
17.	Has the EIA Form been completed (Appendix 1)?	✓
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	✓
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	✓
20.	Is there a plan to i. review ii. audit compliance with the document?	✓
21.	Is the review date identified, and is it appropriate and justifiable?	✓

Sheffield Health and Social Care NHS Foundation Trust

SHSC Guest WiFi: Terms and Conditions

1. Introduction

If you'd like to use our WiFi network, be our guest. In accessing our Guest WiFi, you will be agreeing to our terms of service (detailed in this document). Please read this carefully before accessing the Guest WiFi. Please be aware, the term 'Guest WiFi' used in this document relates to both SHSC Guest and Public WiFi networks.

2. Personal Consent

The SHSC Data and Information Acceptable Use policy governs the use of our Guest WiFi service by all users.

It is your responsibility to ensure the appropriate use of the Sheffield Health and Social Care (SHSC) guest wireless network in accordance with the following terms:

- SHSC does not guarantee the security, confidentiality or the integrity of the user's information on the guest wireless network.
- SHSC is not responsible for the loss, misuse or theft of any information, passwords or other data transmitted by users through the guest wireless network.
- Access to the internet via the SHSC guest wireless network is monitored for inappropriate material and sites which are deemed to contain unsuitable material will be blocked.
- You will be responsible for any internet usage on your guest account and are not allowed to divulge logon credentials to any other person.
- You will not take photos or make recordings of patients, visitors or staff to be uploaded onto any internet-based services without the explicit permission of that person.
- The SHSC Guest Network is not to be used for commercial gain by any user or third party.
- Your access to this service is completely at the discretion of SHSC and your access to the service may be blocked, suspended or terminated at any time for any reason

including, but not limited to, violation of this agreement, actions that may lead to liability for SHSC, disruption of access to other users or networks, or violation of applicable laws or regulations.

- You agree to indemnify SHSC against any claims, demands, actions liabilities, costs or damages arising out of your use of the Service including any material that you access or make available using the Service, or violation of the agreement, including but not limited to use of the Service by you (or permitted by you) involving offensive or illegal material or activities that constitute copyright infringement. You furthermore agree to pay our reasonable legal fees and experts costs arising out from any actions or claims hereunder.

- SHSC may revise these terms at any time and without notice. It is your responsibility to review this policy for any changes.

3. User Risks

- SHSC agrees to provide web content filtering on this service but cannot guarantee that inappropriate sites may not be accessed.

- SHSC assumes no responsibility for the accuracy, timeliness, or appropriateness of materials accessed over the internet.

- The use of this service for illegal, actionable or criminal purposes or to seek access into unauthorised areas is prohibited. Infringement of copyright and software licensing agreements is prohibited.

- Under no circumstances shall SHSC be liable for any direct, indirect, incidental, special, punitive or consequential damages that result in any way from use of or inability to use the service or to access the internet or any part thereof, or user's reliance on or use of information, services or merchandise provided on or through the service, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation, or transmission, or any failure of performance.

- This policy covers the use of the SHSC guest wireless network only. The Trust has no mechanism to control use of personal devices on the public networks and the responsibility for such use lies solely with the individual and/or their parent/guardian.

4. Inappropriate Content

Access to inappropriate content on any SHSC network is strictly prohibited. Inappropriate content includes but is not restricted to:

- Any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory.

- Any obscene or indecent images likely to cause offence, such as pornographic or violent images.

- Any material which is designed to cause incitement, harassment including sexual or racial harassment, thereby causing annoyance, inconvenience or anxiety.

- It is also forbidden to download and store any illegal content such as unlicensed material in breach of copyright laws.

5. Stored Data and Retention

It is required for SHSC to store personal details on the wireless system. Personal details will be securely stored and will not be used for marketing purposes in line with the Data Retention Regulations 2014 and Data Protection legislation.

- Personal details consisting of First Name, Last Name and Email Address will be securely stored.

- Personal details have a retention period of no more than one year before being permanently deleted.

- Requests for information including personal details and internet usage are available upon request.

6. Approval

These terms and conditions were recommended for approval by the Executive Director of Operations and Caldicott Guardian on 30 August 2017.

7. Contact Details

Title	***Name***	***E-mail***
Assistant Deputy Director of Operations & Services	Adam Handley	adam.handley@shsc.nhs.uk