



Sheffield Health  
and Social Care  
NHS Foundation Trust

# Policy:

## IMST 004 - Data & Information Acceptable Use

Executive or Associate Director lead	Executive Director of Finance & SIRO
Policy author/ lead	Assistant Deputy Director of IMS&T (Informatics and Architecture)
Feedback on implementation to	Assistant Deputy Director of IMS&T (Informatics and Architecture)

Document status	Version 1.1
Date of initial draft	18/10/2019
Date of consultation	
Date of verification	11/11/19
Date of ratification	21/11/2019
Ratified by	Executive Directors' Group (EDG)
Date of issue	26/11/2019
Date for review	21/03/2021

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

Keywords	Internet, acceptable use, social media
----------	--

### **Policy Version and advice on document history, availability and storage**

This is version 1.2 of this policy. It replaces the previous version of the Data & Information Acceptable Use policy.

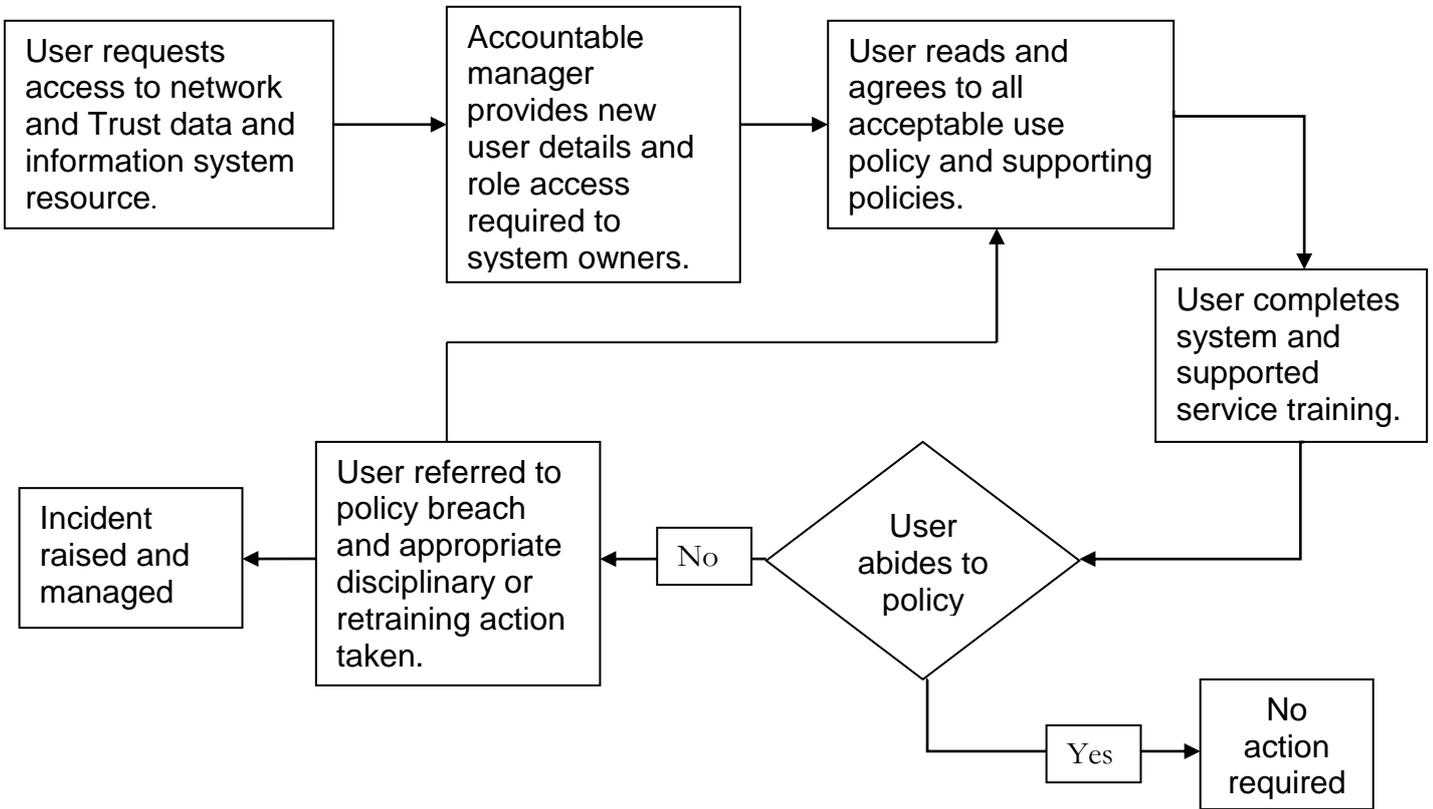
This policy will be available to all staff via the Sheffield Health & Social Care NHS Foundation Trust Intranet and on the Trust's website. The previous Internet Acceptable Use policy will be removed from the Intranet and Trust website and archived.

Revised October 2019

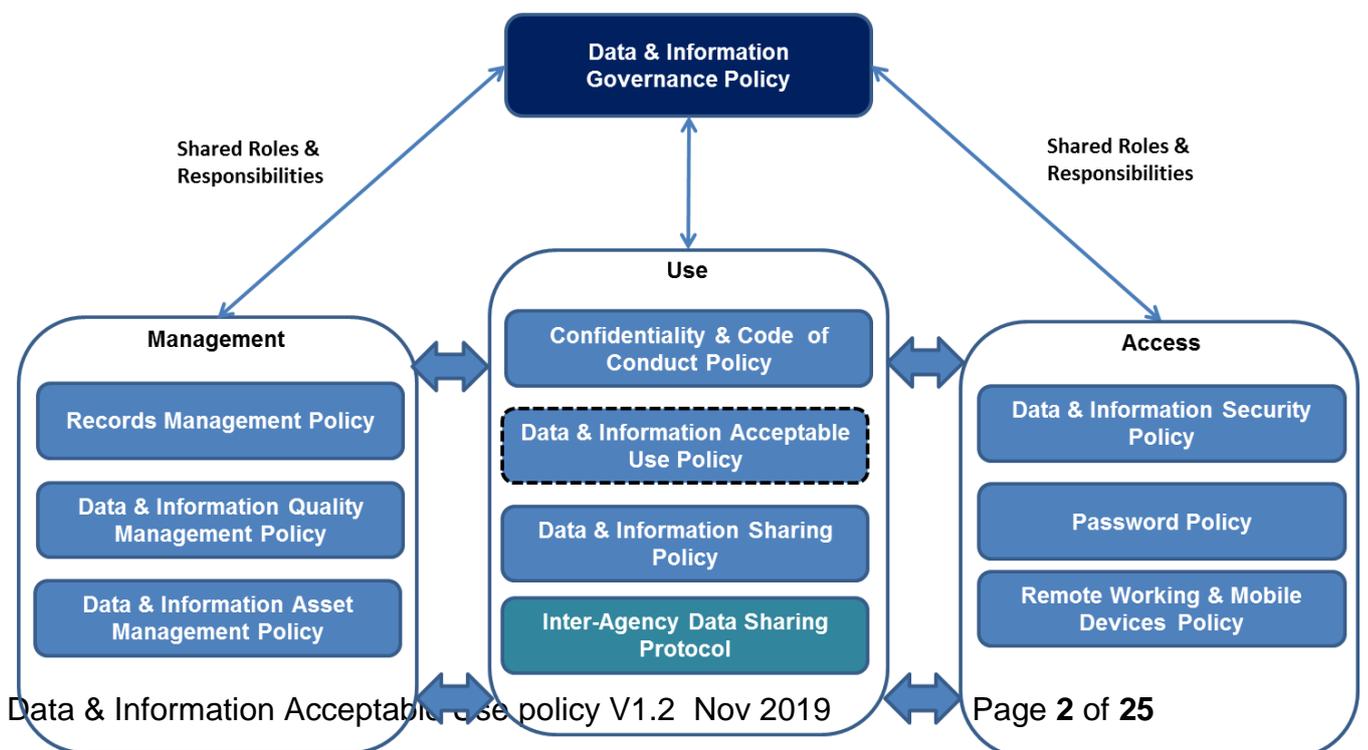
## Contents

Section		Page
	Flow Chart	2
1	Introduction	3
2	Scope	3
3	Definitions	4
4	Purpose	4
5	Duties	5
6	Process	5
	6.1 Adherence to this policy	5
	6.2 Access to and use of electronic systems	6
	6.3 Ensuring integrity of the system	6
	6.4 Monitoring	6
	6.5 User Rights and Responsibilities	7
	6.6 Inadvertent misuse of the Internet	8
	6.7 Use of the Guest Wi-Fi	8
	6.8 Access via govroam	9
	6.9 Social Media (Blogging and Social Networking)	9
	6.10 Email	10
	6.11 Cloud Storage	11
	6.12 Reporting Incidents & Weakness	11
7	Dissemination, storage and archiving	12
8	Training and other resource implications	12
9	Audit, monitoring and review	13
10	Implementation plan	13
11	Links to other policies, standards and legislation (associated documents)	14
12	Contact details	14
13	References	14
Appendices	Appendix A – Version Control and Amendment Log	15
	Appendix B – Dissemination Record	16
	Appendix C – Equality Impact Assessment Form	17
	Appendix D - Human Rights Act Assessment Checklist	18
	Appendix E – Development, Consultation and Verification Record	20
	Appendix F – Policy Checklist	21
	Appendix G – Guest Wi-Fi Terms & Conditions	23

**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 overrules.

## 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 FT (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. 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 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.

### 4. 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.

### 5. 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.

<b>Role</b>		<b>Responsibility</b>	<b>Description</b>
Chief Information Officer	CIO	Director IMST	Responsible for the Information Technology that supports the overarching strategies of the Trust.
Chief Clinical Information Officer	CCIO	Director Medical	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 Nursing	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.
Data Protection Officer	DPO		Supporting Trust - wide Data & Information governance in accordance to GDPR, NHS Digital & England and Data Security and Protection Toolkit

			(DSPT).
Clinical Information Officer	CLIO		Supporting the Chief Clinical Information Officer and trustwide clinical initiatives for increased data and information usage and opportunities, supported by data and information governance framework.
Cyber Security Officer	CSO		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.
Data & Information Asset Owners	DIAO	Directorate	Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems.
Data & Information Asset Managers	DIAM	Service Managers	Primary administrative and management responsibilities for segments of data primarily associated with their functional area
Data & Information Asset Supervisors	DIAS	Supervisors / Team Leaders	Supervisors have responsibility for the day-to-day maintenance and protection of data & information when they are affected by the processes that they manage.
Data & Information Asset Users	DIAU	All Users	Responsibility lies with all staff to make sure that all policies and security measures are adhered to
Data & Information Asset Stewards	DIAS	IMST & Suppliers	Trust and third party IMST enabling and supporting secure & compliant data and information technical implementation, governance and guidance throughout the Trust and in accordance to trust policy, national guidelines and regulations.

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(format to same line)ones) plus other authorised users of systems are required to adhere to this policy.

## 6. Process

### 6.1 Adherence to this policy

Users requiring access to the Trust network and the Internet via Trust facilities will be required to read this policy and sign a declaration that they have read, understood and agreed to abide by its content prior to being granted access.

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.

## **6.2 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.

## **6.3 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 the system.

## **6.4 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.

If any user exceeds a specified limit of time spent on the internet (as agreed by the Executive Management Team), the IT department will notify their manager who will be responsible for investigating the matter. This limit does not define what constitutes acceptable or unacceptable use of the Internet; it serves as a prompt for further action.

Managers 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.

## **6.5 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 Bullying and Harassment 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.

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) 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.

## **6.6 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 Help Desk.

## **6.7 Use of the Guest Wi-Fi**

SHSC provides separate guest Wi-Fi at some of its sites. Anyone using the guest Wi-Fi 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 G.

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 Wi-Fi 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.

## **6.8 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.

## **6.9 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 Corporate Affairs Department. Other members of staff or teams are not permitted to operate open social media accounts for Trust purposes but they may operate closed groups if 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 for Staff” available via the SHSC intranet.

## **6.10 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 Help 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 Help Desk for details of the necessary 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.

### **6.11 Cloud Storage**

Cloud storage should not be used to store or retrieve files containing information about individuals or other sensitive information.

The only exception permitted is in the case of external collaboration, only if no other secure alternative is available. Each exception must be approved through the “Internet Address Access Request” Form, specifying that a cloud storage service is required and provides a reason for access. Requests are assessed on a case-by-case basis and require both line management and IT approval.

Do not use cloud storage for long-term retention of any Trust documents or files. Only use Trust authorised shared network drives and approved methods.

The Trust does not support cloud storage clients or applications.

### **6.12 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.<sup>1</sup>

---

<sup>1</sup> Where any incidents involving suspected fraud are identified, the Trust’s Fraud, Bribery and Corruption Policy should be followed and advice sought from the Local Counter Fraud Specialist ([robert.purseglove@nhs.net](mailto:robert.purseglove@nhs.net)).

- Smartcard or application misuse.
- Smartcard theft.
- Non-compliance of local or national RA policy.
- Any unauthorised access of HSCIC applications.
- Any unauthorised alteration of patient data.

The Trust handles considerable amounts of patient data and this can be 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 Reporting Policy).

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

### **SIRO & Data & Information Governance Group Reporting (DIGB)**

The Data Protection Officer will keep SIRO & DIGB informed of the information security status of the Trust by means of regular reports and immediate alerts where an immediate risk is identified.

### **7. Dissemination, storage and archiving (Control)**

This policy will be made available to all staff via the SHSC intranet. Copies of the previous Internet Acceptable use policy should be removed.

Changes to this policy will be made by the SHSC Information Manager at the request of or approved by the Data & Information Governance Board (DIGB).

### **8. 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.

## 9. Audit, monitoring and review

<b>Monitoring Compliance Template</b>						
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 Manager; Head of Informatics and Information Systems; IT Dept.	Annual	Data & Information Governance Board	Information Manager; Head of Informatics and Information Systems; IT Dept.	Data & Information Governance Board

This policy will be reviewed in March 2021

## 10. Implementation plan

:

Action / Task	Responsible Person	Deadline	Progress update
<i>Upload new policy onto intranet and remove old version</i>	<i>Corporate Affairs</i>	<i>31/03/2018</i>	
<i>Notify adoption of new policy via Trust Connect newsletter</i>	<i>Communications Manager</i>	<i>31/03/2018</i>	

## 11. Links to other policies, standards and legislation (associated documents)

- Social Media Policy for Staff
- Copyright, Designs and Patents Act 1998
- NHS Code of Connection
- Fraud, Bribery and Corruption Policy

## 12. Contact details

<b><i>Title</i></b>	<b><i>Name</i></b>	<b><i>Phone</i></b>	<b><i>Email</i></b>
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
Data Protection Officer	John Wolstenholme	0114 3050749	John.wolstenholme@shsc.nhs.uk

## 13. References

This policy supports compliance with the Data Security and Protection Toolkit available at <https://www.dsptoolkit.nhs.uk/>

## Appendix A – Version Control and Amendment Log

<b>Version No.</b>	<b>Type of Change</b>	<b>Date</b>	<b>Description of change(s)</b>
1	Policy created	March 2018	New policy to replace the previous Internet Acceptable Use Policy as part of a comprehensive review of information governance policies.
1.1	Revision	Apr – Oct 2019	Updates for legislative and monitoring changes and contact details. Clarification on e-mail use.

## Appendix B – Dissemination Record

<b>Version</b>	<b>Date on website (intranet and internet)</b>	<b>Date of “all SHSC staff” email</b>	<b>Any other promotion/ dissemination (include dates)</b>
1	August 2018		

# Appendix C – Stage One Equality Impact Assessment Form

## Equality Impact Assessment Process for Policies Developed Under the Policy on Policies

**Stage 1** – Complete draft policy

**Stage 2 – Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? If **NO** – No further action required – please sign and date the following statement. If **YES** – proceed to stage 3

No. J Wolstenholme, Information Manager, 21 October 2019

This policy does not impact on staff, patients or the public (insert name and date)

**Stage 3 – Policy Screening** - 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 on equality impact assessment for examples and detailed advice. This is available by logging-on to the Intranet first and then following this link [https://www.xct.nhs.uk/widget.php?wdg=wdg\\_general\\_info&page=464](https://www.xct.nhs.uk/widget.php?wdg=wdg_general_info&page=464)

	Does any aspect of this policy actually 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?
<b>AGE</b>			
<b>DISABILITY</b>			
<b>GENDER REASSIGNMENT</b>			
<b>PREGNANCY AND MATERNITY</b>			
<b>RACE</b>			
<b>RELIGION OR BELIEF</b>			
<b>SEX</b>			
<b>SEXUAL ORIENTATION</b>			

**Stage 4 – Policy Revision** - Make amendments to the policy or identify any remedial action required (action should be noted in the policy implementation plan section)

Please delete as appropriate: Policy Amended / Action Identified / no changes made.

Impact Assessment Completed by (insert name and date)

## Appendix D - Human Rights Act Assessment Form and Flowchart

You need to be confident that no aspect of this policy breaches a person's Human Rights. You can assume that if a policy is directly based on a law or national policy it will not therefore breach Human Rights.

If the policy or any procedures in the policy, are based on a local decision which impact on individuals, then you will need to make sure their human rights are not breached. To do this, you will need to refer to the more detailed guidance that is available on the SHSC web site

<http://www.justice.gov.uk/downloads/human-rights/act-studyguide.pdf>

(relevant sections numbers are referenced in grey boxes on diagram) and work through the flow chart on the next page.

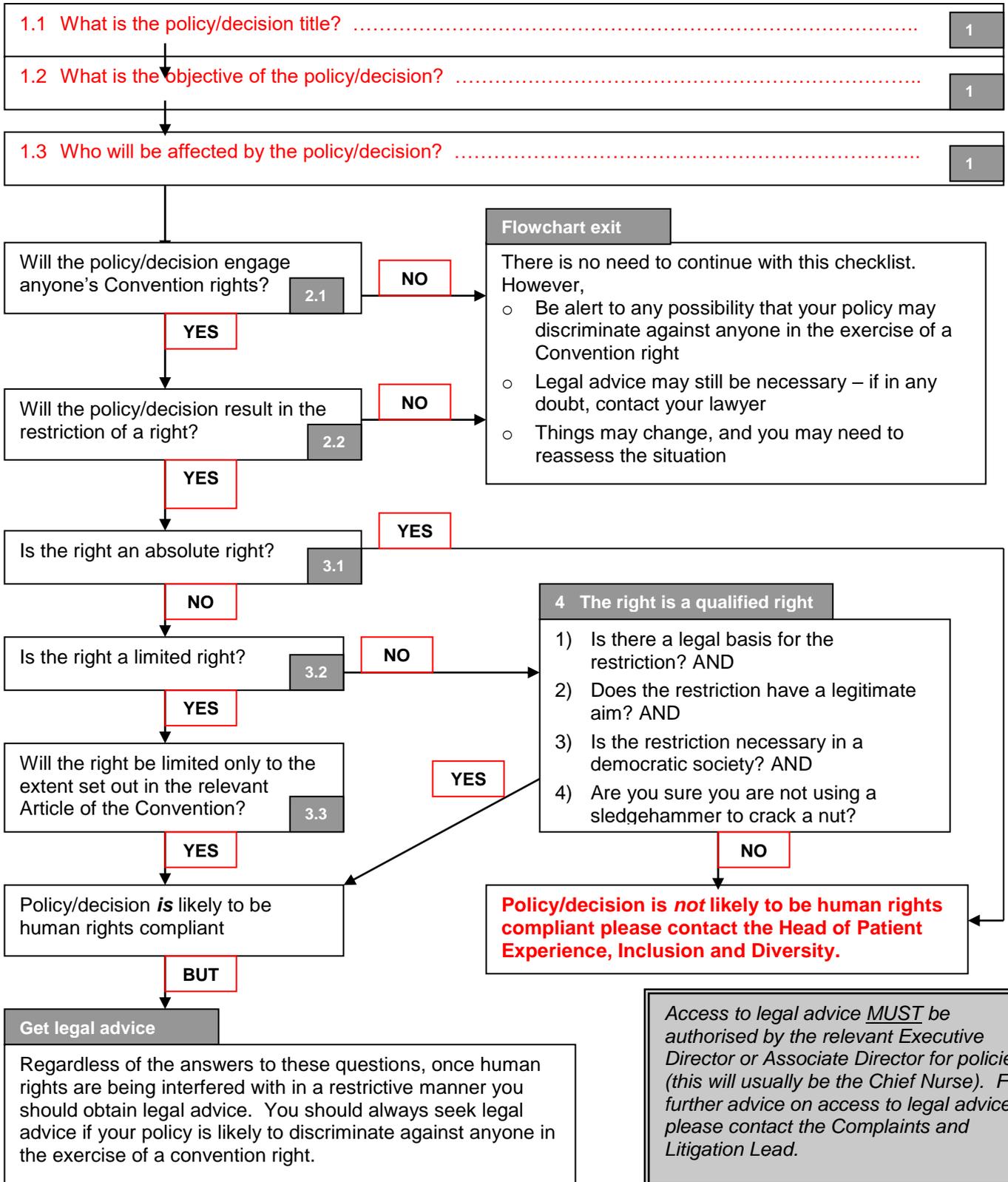
### 1. Is your policy based on and in line with the current law (including case law) or policy?

- ✓ **Yes. No further action needed.**

## Human Rights Assessment Flow Chart

Complete text answers in boxes 1.1 – 1.3 and highlight your path through the flowchart by filling the YES/NO boxes red (do this by clicking on the YES/NO text boxes and then from the Format menu on the toolbar, choose 'Format Text Box' and choose red from the Fill colour option).

Once the flowchart is completed, return to the previous page to complete the Human Rights Act Assessment Form.



## **Appendix E – Development, Consultation and Verification**

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.

## Appendix F –Policies Checklist

***Please use this as a checklist for policy completion. The style and format of policies should follow the Policy template which can be downloaded on the intranet (also shown at Appendix G within the Policy).***

### 1. Cover sheet



All policies must have a cover sheet which includes:

- The Trust name and logo
- The title of the policy (in large font size as detailed in the template)
- Executive or Associate Director lead for the policy
- The policy author and lead
- The implementation lead (to receive feedback on the implementation)
- Date of initial draft policy
- Date of consultation
- Date of verification
- Date of ratification
- Date of issue
- Ratifying body
- Date for review
- Target audience
- Document type
- Document status
- Keywords
- Policy version and advice on availability and storage

### 2. Contents page

### 3. Flowchart



### 4. Introduction



### 5. Scope



### 6. Definitions



### 7. Purpose



### 8. Duties



### 9. Process



### 10. Dissemination, storage and archiving (control)



### 11. Training and other resource implications



### 12. Audit, monitoring and review



This section should describe how the implementation and impact of the policy will be monitored and audited and when it will be reviewed. It should include timescales and frequency of audits. It must include the monitoring template as shown in the policy template (example below).

<b>Monitoring Compliance Template</b>						
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
A) Describe which aspect this is monitoring?	e.g. Review, audit	e.g. Education & Training Steering Group	e.g. Annual	e.g. Quality Assurance Committee	e.g. Education & Training Steering Group	e.g. Quality Assurance Committee

**13. Implementation plan**



**14. Links to other policies (associated documents)**



**15. Contact details**



**16. References**



**17. Version control and amendment log (Appendix A)**



**18. Dissemination Record (Appendix B)**



**19. Equality Impact Assessment Form (Appendix C)**



**20. Human Rights Act Assessment Checklist (Appendix D)**



**21. Policy development and consultation process (Appendix E)**



**22. Policy Checklist (Appendix F)**





# 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 internet 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 be allowed to divulge logon credentials to any other person in compliance with the Digital Economy Act of 2010.
- 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 3G/4G 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 act of 2009 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 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 Clive Clarke as Executive Director of Operations and Caldicott Guardian on 30 August 2017.

## 7. Contact Details

<b><i>Title</i></b>	<b><i>Name</i></b>	<b><i>E-mail</i></b>
IT Infrastructure Team Leader	Adam Handley	adam.handley@shsc.nhs.uk