Sheffield Health and Social Care
NHS Foundation Trust

Proud to care in Sheffield

Policy:

OPS 015 - Mobile Phones, Communication Devices and Internet Access for Service Users

Executive Director Lead	Chief Operations Officer
Policy Owner	Deputy Chief Nurse
Policy Author	Deputy chief Nurse

Document Type	Policy
Document Version Number	Version 2
Date of Ratification	21/07/2020
Ratified By	Audit & Risk Committee (ARC)
Date of Issue	28/07/2020
Date for Review	31/05/2023

Summary of policy
This policy relates to all those who have access to Trust services whether on in-patient units or in community settings. The policy covers service users, carers, relatives, visitors or members of the public.

Target audience	All service users, carers/relatives, visitors and members of the public using mobile phones or other communication devices while on Trust premises. List those staff who should read this policy

Keywords	Mobile, phone, tablet, device, communication, internet

Version 2 of this policy is stored and available through the SHSC intranet/internet. This version of the policy supersedes the previous version (V1 October 2016). Any copies of the previous policy held separately should be destroyed and replaced with this version

Version Control and Amendment Log (Example)

Version No.	Type of Change	Date	Description of change(s)
1.0	Approval and issue	October 2016	Amendments made during consultation, prior to ratification.
2.0	Review / approve / issue	May 2020	Early review undertaken to update the policy to in order to comply with new regulatory requirements.

Contents

1 Introduction

Communication with family and friends is an essential element of support and comfort for people using our services, particularly on the in-patient wards. Modern technology has made communication relatively easy, particularly with the widespread use of mobile phones, text messaging and e-mailing. Mobile phones commonly also have extended functions such as camera and video recording, music playing capability, and internet access.

The purpose of this policy is not to reduce the opportunities for communication but to consider the risks associated with the ever increasing array of communication devices.

It is important to find a balance between the needs of service users, for example:

- Promoting positive contact with carers, friends and relatives;
- Providing a therapeutic environment;
- Protecting the rights of individuals;
- Protecting people from abuse;
- Promoting recovery;
- Protecting confidentiality;
- Promoting acceptable standards of behaviour;
- Maintaining communications and contact with family and friends while safeguarding against the inappropriate use of such devices.

Primary concerns relate to the use of the camera, audio and filming facilities on mobile phones with can threaten both personal and organisational security, including the privacy of both service users and staff.

Mobile phones and computing devices provide a readily available means of communication with family and friends and are in widespread use. Many service users, voluntary or detained, are therefore likely to have one. It is unlikely to be appropriate to impose a blanket restriction banning their use except in units specifically designed to provide enhanced levels of security in order to protect the public. Moreover, blanket restrictions may breach Article 8 of the Human Rights Act 1998.

2 Scope

This policy relates to all those who have access to Trust services whether on in-patient units or in community settings. The policy covers service users, carers, relatives, visitors, external contractors or members of the public.

3 Purpose

The Trust has a legal obligation to respect the private lives of service users, staff and the public, maintaining their safety, privacy, dignity and confidentiality and all information relating to them. The Human Rights Act (HRA) 1998 enshrines the right to respect for private and family life as set out in Article 8 of the European Covention on Human Rights. The Act makes it unlawful for public authorities (including NHS Trusts) to act in a way which is incompatible with the Convention.

The purpose of this policy is to:

- Identify the appropriate use of mobile phones and communication devices on Trust premises, ensuring that contact with family and friends is maintained in a way that does not intrude on the safety and wellbeing of others;
- Identify situations and conditions where it would be appropriate for staff to restrict access to mobile devices, for example, medical grounds, breaches of confidentiality, privacy or respect of others;

Identify the appropriate access to the Trust's infrastructure and the use of the internet to support communication and recovery.

4 Definitions

Mobile phone is defined as a hand held device, sometimes also known as a smart phone, which is connected to a wireless telecommunication network allowing the user to send and receive calls and text messages; it may also link to the internet.

Tablet is a wireless, portable personal touch screen computer which is bigger than a smart phone but typically smaller than a notebook or laptop. It has the capability of connecting to the internet independently using a wireless telecommunication network or Wi-Fi.

Service User is any person voluntarily or compulsorily in receipt of a service from the Trust, who may be on an in-patient ward, in a residential setting, or attending out-patient areas or day services.

MHA is an abbreviation of the Mental Health Act 1983.

CoP is an abbreviation of Code of Practice (for the purposes of this policy, the Code of Practice relating to the Mental Health Act 1983.

HRA is an abbreviation of the Human Rights Act 1998.

MDT is an abbreviation of multi-disciplinary team - a group of clinicians from different disciplines working together.

5 Detail of the policy

The aim of this policy is to recognise the concerns that may arise about the inappropriate use of mobile phones, communication device and internet access for services users whilst in our care premises. The policy aims to encourage and facilitate there use whilst safely managing any associated risks.

6 Duties

Managers must ensure that the areas of the Trust for which they have responsibility display clear notices for service users, relatives/carers and members of the public setting out the Trust's expectations in relation to the appropriate use of mobile phones and other communication devices.

7 Procedure

7.1 Common use

Mobile devices are a valuable tool in maintaining contact and communication with friends and family, and are particularly important to service users on in-patient wards. However, these devices should always be used discreetly so as not to disturb/impact on others. On in-patient wards it may be reasonable to require mobile phones and tablet devices to be used in quiet or silent mode, with headphones or switched off in key areas e.g. quiet rooms and sleeping areas. Their use may be restricted to designated areas, for example, in day rooms or activity rooms on in-patient wards and in reception areas only in other services e.g. community mental health teams, therapy services etc.

7.2. Associated risks

Mobile phones, tablets and other electronic devices commonly have functions capable of visual and audio recordings, filming on mobiles/tablets and may also provide easy access to the internet. However, the misuse of communication devices has given rise to a significant number of cases relating to inappropriate use, especially in relation to the contravention of the right to privacy.

Anyone found using their mobile phone to make audio recordings or taking photographs of other services users, visitors, staff or images of Trust premises will be asked to delete the images/recording, without consent. They must do so in the presence of staff. Staff may need to assess service users' capacity to consent when these incidences occur.

7.3 Restriction of use – in-patient wards

It may be appropriate in certain circumstances to confiscate mobile phones or mobile computing devices in cases where service users are unable to comply with this policy or where the clinical team believe that access to the internet may not, at that time, be in the service user's best interests. Where it is necessary to confiscate a device, this must be a temporary measure only and the rationale for confiscation must be fully documented in the patient record. In order to avoid contravention of Article 8, the confiscation must be reviewed every twenty-four hours – the rationale for the continuation of the confiscation must be recorded on each occasion, as must the decision to return the device to its owner.

In secure in-patient settings, for example, Forest Lodge and Endcliffe Ward, individual risk assessments will be undertaken within twenty-four hours to ensure that access to a mobile phone or tablet is in the best interests of the service user.

Where staff believe that a visitor is breaching the terms of this policy they have authority to ask the visitor to hand the device to staff for safe keeping for the duration of their visit. Failure to do so will result in the visitor being asked to leave Trust premises.

Where a service user, relative/carer or visitor has a disability and they use a mobile device to meet a need associated with the disability (for example, they may use a live British Sign Language interpreting service via an App or use a mobile device to increase text size on electronic documents), the mobile device must only be removed in exceptional circumstances; the impact of the removal in such circumstances must be considered in light of the support being required by/provided to the individual in relation to their disability and alternative options should be considered in supporting their communication needs.

7.4 Storage of confiscated mobile phones and other communication devices

When a device is confiscated it will be stored by staff in a secure, lockable cabinet on Trust premises. On return of the device, the owner will be asked by staff to sign to confirm its return.

7.5 Internet access on in-patient wards

Service users' mobile phones and tablets are able to connect to the Trust Guest Wi-Fi.

A number of laptops are available on in-patient wards for the purpose of allowing service users access to the internet. Staff will ensure that access is appropriate. Any inappropriate access will result in the service user being denied access.

7.6 Use of Trust provided devices

At times it will be appropriate for the Trust to provide communication devices for use by a Service User. This should be used in line with this overall policy, supported by the terms and conditions of the use of 'Guest Wi-Fi where a connection is required (**Appendix C**). Where a Trust device is provided for a Service User, its use will be monitored by Trust staff. Any accounts accessed by the service user (including but not limited to email, video / call applications) should be signed out and closed down prior to it being provided to another user.

7.7 Inappropriate access

- The Trust reserves the right to prevent access to any internet sites it considers inappropriate,
- When accessing the internet, either using the Trusts systems or the service users own data. users must not:
  - Use the internet for any purpose that conflicts with any Trust Policy, Code of Conduct.
  - Use the internet to create, hold, transmit or view material that has an obscene, pornographic or sexually offensive content.
  - 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.
  - Use the internet to make untrue, inaccurate, misleading or offensive statements about any person or organisation.
- The Trust monitors use of the internet in line with legislation 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.
- All internet activity on Trust systems is logged automatically and audited periodically.
- Monitoring will be carried out in accordance with legislation such as the Regulation of Investigatory powers Act 2000, the Data Protection Act 1998, the Human Rights Act 1998 and Trust policy regarding monitoring and privacy.

7.8 Video calling

Some applications, for example Skype and Facetime are valuable tools in helping service users maintain contact with their family and friends, especially when they are on in-patient wards. Wherever possible this should been undertaken within a private area of the ward. Staff should encourage and support service users to access these applications when it is considered to be in their best interests to do so. Any

restriction on the use of these applications must be recorded in the patient record and must be reviewed every twenty-four hours.

7.9 Safeguarding

SHSC will safeguard and promote the welfare of service users' information and to prevent inappropriate photographs being taken of either the individual concerned or of confidential information pertaining to them. Any breaches must be referred to the Trust Safeguarding Team.

7.10 Infection Prevention and Control

All staff to encourage services users to clean mobile devices after use to prevent spread of infection.

8 Development, consultation and approval

This policy has been reviewed following consultation with Tony Bainbridge, Deputy Director of Nursing (Operations) via the Clinical Operations meeting, Sunrise Service User Group, Nick Gillot Deputy Director IMST and Anita Winter, Head of Patient Safety on behalf of the Service User Safety Group.
The following changes were made as the result of consultation;

The changes/amendments made are as follow;

- 1 - Audio and filming added.
- 2 – external contractors added
- 3 – handheld added
- 7.1 – headphones added
- 7.2 – filming on mobiles/tablets, capacity to consent and without consent added
- 7.3 – risk assessment review within twenty four hours added
- 7.5 – Service users are able to connect to the Trust's Guest Wi-Fi
- 7.6 – Use of Trust provided devices added
- 7.8 – privacy added
- 7.9 – Safeguarding section added
- 7.10 – Infection, Prevention and Control added
- Appendix C- Terms and Conditions for Guest Wi-Fi

9 Audit, monitoring and review

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
Policy content, including duties and process.	Review of policy	Policy Lead	3 yearly, or before to meet regulatory or statutory requirements	Deputy Chief Nurse	Service User Safety Group	Service User Safety Group

This policy will be reviewed every three years or earlier if legislation dictates or practices change. The policy review date is 31 May 2023

10 Implementation plan

- This policy will be implemented via the management structures within the relevant services/ directorates.
- New staff should be made aware of this policy and potential restrictions of the use of mobile devices by their managers.

Action / Task	**Responsible Person**	**Deadline**	**Progress update**
Upload new policy onto intranet and remove old version	Deputy CEO	*TBC*	*Completed TBC*
A communication to be issued for team briefings	Communications team	TBC	*On agenda for team meeting TBC*
A communication to be issued to education, Training and Development to review training	Communications team	*TBC*	*On agenda for team meeting TBC*
Make team aware of new policy	Team Managers		*To be discussed in team briefings*

11 Dissemination, storage and archiving (Control)

A copy of this policy is available to all staff via the Trust intranet. All staff should familiarise themselves with this policy and managers should ensure that appropriate signage in relation to the use of mobile communication devices is clearly visible on all Trust premises. All previous versions of this policy will be removed and any paper copies to be destroyed.

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1.0	October 2016	October 2016	October 2016	N/A
2.0	July 2020	July 2020	20/07/2020	N/A

12 Training and other resource implications

Service Directors, Assistant Service Directors, Service and Team Managers are responsible for making sure that their staff are aware of and comply with this policy

13 Links to other policies, standards (associated documents)

Mental Health Act 1983
Mental Health Act Code of Practice (2015)
Human Rights Act 1998 – Article 8
Safeguarding Adults and Prevent Policy
Infection Prevention and Control Policy
SHSC Guest Wi-Fi Terms and Conditions.

14 Contact details

Title	***Name***	***Phone***	***Email***
Deputy Chief Nurse	Brenda Rhule		brenda.rhule@shsc.nhs.uk
Deputy Director of Nursing (Operations)	Tony Bainbridge		anthony.bainbridge@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: Brenda Rhule 28th April 2020	**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 – Human Rights Act Assessment 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?**

X **Yes. No further action needed.**

☐ **No. Work through the flow diagram over the page and then answer questions 2 and 3 below.**

2. **On completion of flow diagram – is further action needed?**

X **No, no further action needed.**

☐ **Yes, go to question 3**

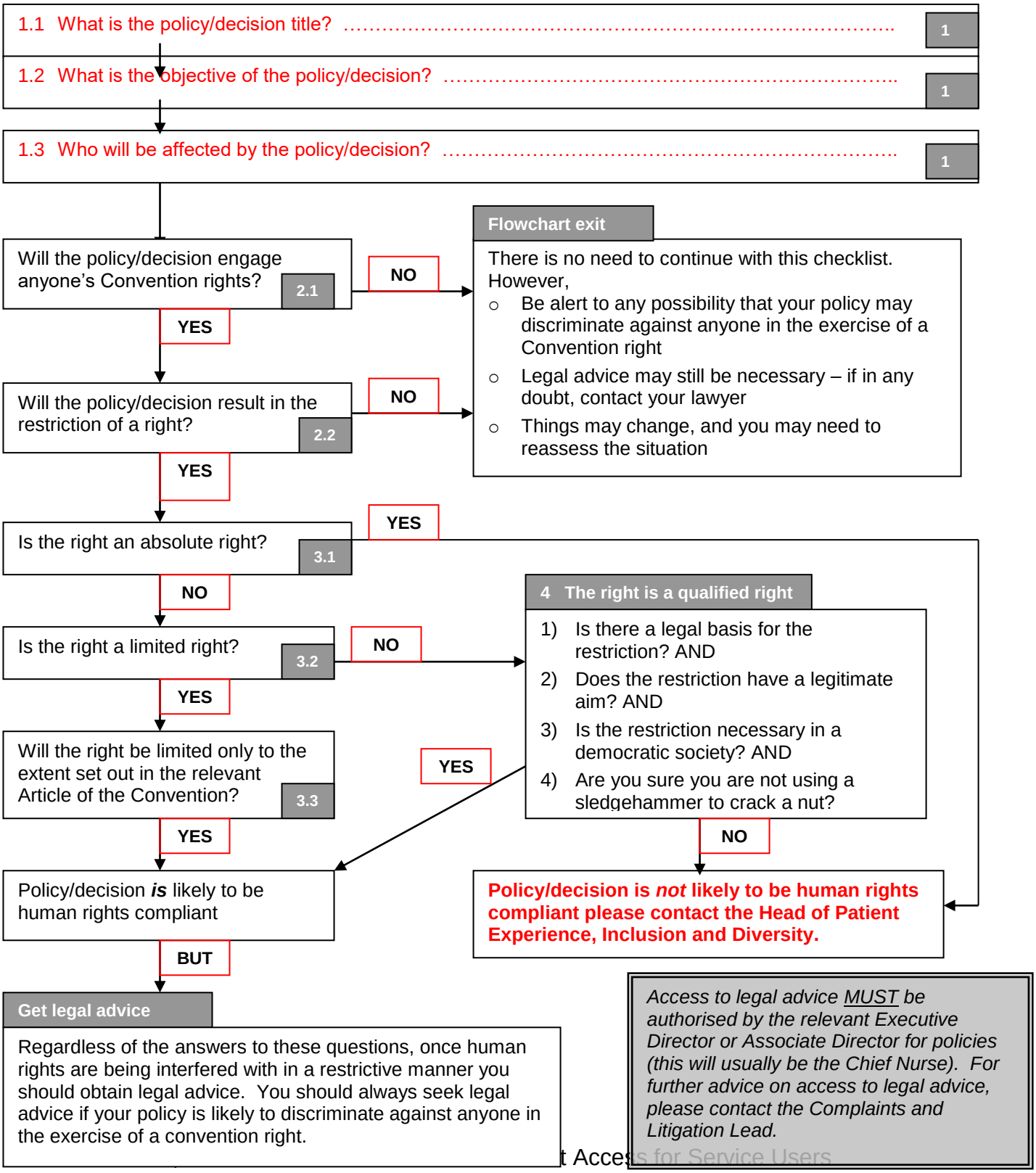
3. **Complete the table below to provide details of the actions required**

Action required	By what date	Responsible Person

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 C

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 the Data Protection Act 1998.

- 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.