INTERNET ACCESS FOR SERVICE USERS

Including the Use of Mobile Devices within Inpatient Settings

Policy number and category	**C42**	**Clinical**
Version number and date	**5**	**March 2025**
Ratifying committee or executive director	**Trust Clinical Governance Committee**	
Date ratified	**May 2025**	
Next anticipated review	**May 2028**	
Executive director	**Executive Director of Quality & Safety**	
Policy lead	**Chief AHP / Associate Director for Recovery, Experience, Spiritual Care & Physical Health**	
Policy author *(if different from above)*		
Exec Sign off Signature (electronic)	*M Halley Green*	
Disclosable under Freedom of Information Act 2000	**Yes**	

POLICY CONTEXT

- The Trust acknowledges the importance of internet access in everyday life and aims to support access for service users, carers, and visitors where it is safe to do this.
- The Trust is committed to providing access to the internet and other information technology to support service users in their recovery.

POLICY REQUIREMENT – see Section 2

- Computing facilities will be provided to allow internet access.
- This policy requires that local service areas consider the need for additional local guidelines to support this policy.
- Where mobile devices are allowed, there will be guidelines for their use by service users, carers, and visitors.
- Use and access will be identified for each service user in accordance with local guidelines and in identified areas an internet passport will be provided. This will specify levels of supervision required.

> • There will be four levels of access for service users via the Trust provided equipment.

Change Record

Date	Version	Author (Name & Role)	Reasons for review / Changes incorporated	Ratifying Committee
March 2025	5	Kirstie Jones, Chief AHP / Associate Director for Recovery, Experience, Spiritual Care & Physical Health	Three Yearly Review	Trust CGC

CONTENTS

1. INTRODUCTION

1.1. Rationale

The Trust acknowledges the importance of internet access in everyday life in line with modern human rights and aims to support access for service users, carers and visitors where it is safe to do so and least restrictive practices can be used

Mobile devices (smartphones, tablets, and laptops) are increasingly used within services. While beneficial, they present challenges, particularly in inpatient areas. This policy outlines procedures to maintain safety while reducing unnecessary restriction

A separate network with safeguards, firewall protection and filters is provided for service user use. **Under no circumstances must service users be given access to Trust NHS networked computers, regardless of supervision level.*

All Trust staff must comply with the NHS Confidentiality Code of Practice (2003) and relevant terms of employment.

1.2. Scope

This policy outlines procedures for providing internet access to service users using Trust-provided or personal mobile devices.

It clarifies the application of this access and highlights local service responsibilities to ensure safe, equitable and structured use.

It applies to

- All inpatient staff, particularly nurses and occupational therapists
- Staff supporting IT or security
- Estates and support teams

This policy does not apply to HMP Birmingham

1.3. Principles (beliefs)

1.3.1 Service users, carers and visitors of modern mental health services have an expectation that they should have access to the internet where it is appropriate to do so.

1.3.2 The Trust supports access to the internet via mobile devices and Trust provided equipment. However, in order to maintain its duty of care the Trust

retains the right to restrict access to either mobile devices or Trust equipment for individual service users.

1.3.3 Staff will understand the key components of data protection and will support service users to ensure the safety of themselves and others.

1.3.4 For service users who are inpatients, supervising staff have a responsibility to monitor both the access and material viewed at a level which is appropriate to the service area or individual.

1.3.5 Inappropriate material, which falls under the following categories, is explicitly prohibited.

- Pornography

- Paedophile materials or literature

- Hate sites or anything which could have terrorist associations.

  If attempts are made to view such material staff will intervene to prevent this in the following ways.

- In the case of service users, access to mobile devices or Trust computers will be revoked (mobile devices will be removed until clinical team review and/or sites will be blocked by the ICT department.)

- In the case of carers or visitors, if requests to refrain from access are ignored, they may be asked to leave the inpatient setting.

- Staff are to complete an eclipse form in the event of one of the above occurring.

1.3.6 The user should not attempt to connect or use any secured or unsecured wired or wireless network/s to gain unauthorised access to any data or internet services. This is applicable to both personal and Trust issued devices.

1.3.7 If service users view sites which indicate terrorist philosophy and a potential threat the appropriate clinical team is responsible for reporting this.

1.3.8 This policy relies on the need for local service areas to provide additional guidelines to reflect the needs of their individual service.

2. **POLICY**

2.1. Service User access via Trust provided equipment or use of personal mobile devices.

2.1.1. Computing facilities will be provided to allow internet access. This access will support service user's recovery to further social, communication, education, and vocational goals.

2.1.2. Trust provided equipment will be in designated activity and ward areas where it is appropriate.

2.1.3.   Service wide access will be managed via categories. There will be 4 categories of access afforded; Service areas will decide which is most suitable for service users based upon capacity, risk assessment, and the balance of risk/benefit to the service user and members of the public. The levels are.

- A – Open

- B – Restricted

- C – Open (no shopping)

- D – Video Conferencing Only (e.g., Teams, Zoom)Note: Skype is now obsolete; video access should occur via Microsoft Teams, Zoom, or other secure platforms approved by the Trust.

Access categories are enforced by the IT department. Requests to unblock sites can be submitted to the Chief AHP.

Service users will be informed of access levels on admission and may be issued an internet passport reflecting supervision requirements.

Inappropriate material (e.g., pornography, hate sites, terrorist content) is strictly prohibited. Attempts to access such content will lead to revoked access and an Eclipse incident form submission

Radicalisation/Prevent: If service users access or attempt to access radicalising or terrorist content, staff must follow safeguarding procedures and escalate through the Prevent process.

These categories are enforced by the Trust IT infrastructure.
(*Details of access within the categories can be found in the appendix 11.1*)

The sites which are available will be reviewed; requests to unblock specific sites can be made via the Chief AHP / Associate Director for Recovery, Experience, Spiritual Care & Physical Health

2.1.4   On admission each individual service user will be made aware of their level of access to the internet as part of the admission process.

Local guidelines may dictate the use of an internet passport (a copy can be seen in appendix 10.4). This will indicate the level of access each individual has and the supervision arrangements ie 1:1 constant, 1:1 intermittent or group. This will ensure that both the individual service user and members of staff are clear about the level of access granted. The passport will be updated following review.

2.1.5   It is the responsibility of all staff to ensure that the service user has been informed and understands safe internet use in particular the need for confidentiality. Some inpatient units may provide internet safety groups and have contracts in place for the use of these. Service users will be made aware that smart phones may have a GPS tracking device within certain applications which they may wish to disable.

2.1.6   In the event that service users exceed their level of access or do not follow rules in relation to confidentiality access to the internet will be suspended.

Staff will use discretion to manage such suspensions in the same way as other restrictions and contraband are managed. Staff should take reasonable steps to manage this and to escalate this to senior staff where required. The management of this should be documented using an eclipse form.

2.2. Access to the internet for carers or visitors in inpatient areas using personal mobile devices

2.2.1.   Staff will ensure that carers and visitors to inpatient units are informed and understand the need for safe internet use. These messages will be supported by leaflets and posters displayed in the inpatient area.

2.2.2   If staff members become aware that these rules are not being followed and use of the internet is presenting a risk to service users in our care or others, the carer or visitor will be asked to refrain. If they choose not to do this, they will be asked to leave the unit.

2.2.3.   Staff will use their discretion in managing incidents where service users are placed at risk. Staff should take reasonable steps to manage this and to escalate this to senior staff where required. The management of this should be documented using the Eclipse.

3.   PROCEDURE

Procedure for service users using Trust provided equipment.

3.1   Access

3.1.1   Access to computer facilities will be provided to service users in accordance with available resources.

3.1.2   Each local service will be required to evidence availability of internet access and to ensure fair provision for all service users.

3.1.3   Prior to internet access each service user will be aware of the categories of access and the categories which they are permitted to use. In identified clinical settings service users will be provided with their own internet passport (appendix 10.4) which states the level of access granted and the level of supervision required. The level of supervision will be determined by individual need and the service area in which the service user is being cared for.

3.1.4   Where service users are provided with an internet passport, he/she will be required to sign a copy of this document which will outline their responsibility whilst using the internet.

3.1.5   Additional levels of supervision and support may be required for any Service User who is high risk; it is the responsibility of the clinical team to inform staff of the level of supervision required. In some cases, additional unit staff may need to accompany services users during internet sessions.

3.2 Restrictions

3.2.1 With sufficient clinical justification service areas and clinical teams may restrict access in particular settings and / or for individuals. In these instances, it is important that the rationale is clearly captured within either a local guideline or in the individual's care plan/ internet passport and that this is explained to the service user/s.

3.2.2 In determining access the service user's capacity and potential risk shall be considered. Where possible, steps to mitigate against potential risk will be put in place to facilitate access.

3.2.3 Initial assessment for groups or individuals will establish any issues or risks, such as assistance with technical skills or tendency to access inappropriate material. The selection of access levels can be used to minimise risk, the categories will provide a range of access but in all categories inappropriate URL's will be blocked through the central mechanism of maintaining safe and therapeutic computer access. Known risks and interests in violent, pornographic, or other inappropriate material will be highlighted and recorded in the clinical records.

3.2.4 The outcome of the initial assessment and on-going review (including supervision requirements) will be documented in the progress notes and arrangements highlighted in the care plan. Changes in access levels will be communicated to the wider staff group during clinical meetings and handovers.

3.3 Use and supervision

3.3.1 In some clinical settings there will be minimal restriction to use of the internet. This will be agreed locally, and service users made aware of access and agreement of use on admission.

3.3.2 Where in use the internet passport will identify the level of supervision required for each individual the levels of supervision will consist of.

- Group
- Casual / intermittent
- Close 1:1 at all times

3.3.3 For all Trust equipment, even that with more open access, staff will be required to log in for a service user each time they use the internet. Access will be dependent on the individual's categories of access identified within the local agreements or in the internet passport.

3.3.4 Local guidelines will detail the procedure for log in and maintenance of log in pass codes. Passwords will be changed on a regular basis.

3.3.5 Staff members will prepare the room and ensure that service users do not have access to the log in codes.

3.3.6 Local guidelines will consider the need for local records of internet use.

3.3.7   All areas should conduct random check on Trust computer histories to monitor for access to restricted sites.

3.3.8   The Trust internet filter retains history of internet use for up to a year. This data is available on request.

3.3.9   Service users may not download software of any kind. Other information may be downloaded with the consent of the supervisor (e.g., articles for study purposes).

3.3.10   Where a computer is not connected to a printer, staff will have the opportunity to obtain encrypted USB memory sticks for service users so that the files can be transported for printing where this is permissible and reasonable.

3.3.11   Gambling online will not be permitted.

3.3.12   Misuse of Internet access will lead to termination of the session and suspension of access pending discussion with the clinical team.

3.3.13   Withdrawal of internet access will not be used as a punitive measure under any circumstances. Access will only be withdrawn if the policy or local guidelines have not been followed, and a risk is presented.

3.3.14   Use of video contact i.e. via Skype, Zoom or Teams will be encouraged if deemed safe by the clinical team. The team will need to consider issues of safeguarding and rules of use, to include the need to end a video visit if the rules are not followed. Consideration for children/ vulnerable people at the other end of the video call will be required.

There will be a user category which only includes video contact ie skype. This is to guard against use without staff knowledge. A leaflet will be provided (and poster displayed) providing general information to detail safe use of video visits. This will emphasise the need to ensure log out after the session is finished.

3.4   Security

3.4.1   Trust computer equipment will be secured and logged out when not in use.

3.4.2   All computer equipment will bear a Trust asset reference.

3.4.3   Any data stored on computers must be considered vulnerable to corruption, deletion, or abuse and therefore, under no circumstances, should important or sensitive information be retained on the hard disk.

3.4.4   All computers designated for service users will have anti-virus and internet control software installed.

3.4.5   All computers will run Trust-approved licensed software only

3.5   Incident Reporting

3.5.1   Any suspected / actual breaches of the requirements set out in this policy or misuse of facilities by service users must be reported to the unit manager, clinical teams and reported in accordance with the **Trusts Incident Reporting and Management Policy (R&S 02).**

A summary of the procedure for Trust provided equipment.

When a service user is admitted on to the ward, and would like to access the internet using trust equiptment, an agreement will need to be made by the clinical team.

The clinical team will need to decide upon what level of access a service user will be most suitable; taking into account capacity and risk history.

Additional levels of supervision may be required for any service user who is high risk.

The level of access and supervision level will be documented in the clinical note

For each service user computer session staff are required to:

- prepare the room

- log on to the computer with the correct user name dependent on the level of access the service user has

- ensure that service users do not have access to log on codes

Misuse of internet access will lead to termination of the session and suspension of access pending discussion with the clinical team

Eclipse form will be required

Ongoing review of the use and level of internet access using trust equipment to be carried out by staff and documented in clinical record.

3.6 Procedure for access using own mobile devices.

3.6.1 Access

In identified areas service users will retain access to their own mobile devices ie tablets and smart phones. This will be clear within local guidance and agreement on use will be identified and communicated to service users upon admission, this may include the use of contracts to determine boundaries in internet access.

Where patients and/or their relatives, friends or visitors have access to their own mobile devices or tablets, it is not permitted under any circumstances for these devices to be used to take photographs, film, or record other service users or staff in any area. Please refer to the Audio and Visual Recording by Patients Policy.

3.6.2 Restrictions

3.6.2.1 With sufficient clinical justification service areas and clinical teams may restrict access in particular settings and / or for individuals. In these instances, it is important that the rationale is clearly captured within either a local guideline or in the individual's clinical record and that this is explained to service user/s. It is also important that the service user (if applicable) is given information on what would need to be seen from them for restricted access to be re-considered by the clinical team.

3.6.2.2 In determining access the service user's capacity and potential risk shall be considered. Where possible steps to mitigate against potential risk will be put in place to facilitate access.

3.6.2.3 The outcome of the initial assessment and on-going review will be documented in the main clinical record.

3.6.3 Use and supervision

3.6.3.1 Misuse of internet access will lead to immediate removal. This may be via removal of a mobile device and suspension of access pending discussion with the clinical team.

3.6.3.2 The trust is committed to encompassing least restrictive practice and under no circumstances will access be terminated for reasons other than abuse of the policy and criteria for access. It should not be seen that withdrawal is a punitive measure under any circumstances.

3.6.3.3 Use of video contact, i.e. via Teams / Zoom / Facetime, will be supported if deemed safe by the clinical team. The team will need to consider issues of

- Safeguarding
- Rules of use, to include the need to end a video visit if the rules are not followed.
- Consideration for children/ vulnerable people at the other end

- The required levels of supervision/support
- Potential risk

3.7 Security

3.7.1 Mobile devices are the responsibility of the owner.

3.7.2 Service Users are to be made aware of protecting others privacy through discussion with staff and the use of information posters on the ward.

3.8 Incident Reporting

3.8.1 Any suspected / actual breaches of the requirements set out in this policy or misuse of facilities by service users must be reported to the unit manager, clinical teams and reported in accordance with the **Trust policy.**

A summary of the procedure for use of mobile devices in inpatient settings

In identified areas service users will be able to retain their mobile devices i.e. tablets and smart phones.

↓

Agreement of use will be clarified upon admission (see local guidance).

↓

A capacity test or clarification of risk history in relation to the use of mobile devices will need to be used where approriate.

↓

Outcome of inital assessment to be documented in clinical record.

↓

Misuse of internet access will lead to immediate removal and suspension of access pending clinical team discussion.
Eclipse form will be required

↓

Ongoing review of the use of the mobile device to be carried out by staff and documented in clinical record.

4. RESPONSIBILITIES

Post(s)	Responsibilities	Ref
All Staff	To be aware of and to adhere to the policy	
Staff supervising service users	• Ensuring service users are aware of their level of access and have a passport if in use in the clinical setting. • Have knowledge of the policy and to follow local guidelines regarding records of use. • To supervise Service Users as indicated by their level of access. • Supervision and security of equipment. • Reporting equipment malfunction immediately to IT. • Reporting incidents relating to service user PC use. (**Trust Incident Reporting Policy**) Manage and keeping confidential the log on information necessary for internet access. • Informing and advising service users	
Service, Clinical and Corporate Directors	• Development of the local protocol. • Ensuring that staff are informed of the policy and local guidelines to facilitate safe access to the internet for service users, carers and visitors. • Monitoring compliance with this policy • Ensuring that agreed websites are requested to be unblocked with ICT at a local level.	
Policy Lead	• To review the policy at the agreed interval	
Executive Director	• The Chief Executive is accountable for ensuring that there are systems and processes in place to ensure the safety, confidentiality, and integrity of computing facilities for service users in BSMHT. This responsibility may be delegated to appropriate executives. • The Executive Medical Director is the Caldicott Guardian.	
Service Users	• Use internet access within agreed parameters. Maintain confidentiality and safety. Participate in access reviews and follow policy rules.	

5. DEVELOPMENT AND CONSULTATION PROCESS

Consultation summary	
Date policy issued for consultation	March 2025
Number of versions produced for consultation	1
Committees or meetings where this policy was formally discussed	
PDMG	

Where else presented	Summary of feedback	Actions / Response
PEAR	No feedback noted	
CGC	No feedback noted	

6. REFERENCE DOCUMENTS

6.1 Data Protection Act 2018

An Act to make provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information

6.2 Computer Misuse Act 1990

UK law passed in 1990 that made it illegal to hack into computers. The Act Introduced three new offences: unauthorised access to computer material (for example out of curiosity), unauthorised access with intent to facilitate the commission of a crime (for example fraud or blackmail), and unauthorised modification of computer material (for example to introduce a virus).

6.3 NHS Confidentiality Code of Practice 2003

The NHS Confidentiality Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their health records It replaces previous guidance. HSG(96) 18/LASSL (96(5 - The Protection and Use of Patient Information, and is a key component of emerging information governance arrangements for the NHS.

7. BIBLIOGRAPHY

None

8. GLOSSARY

None

9. AUDIT AND ASSURANCE

Element to be monitored	Lead	Tool	Freq	Reporting Committee
Review of local guidance	Clinical Directors,		Annually	Local Governance
Access to the internet	Lead for service user, carer, and family experience	Service user feedback	Minimum review date will be Sept 2024	Patient Experience and engagement group.
Review of incidents	Chief AHP & Associate Director for Recovery, Experience, Spiritual Care & Physical Health	Eclipse	Minimum review date will be Sept 2027	IGSG
Review of IG incidents to include Sample check of wards for posters and guidance information	Head of Information Governance	Information Governance Site Audits	Minimum review date will be sept 2027	IGSG

10. APPENDICES

10.1 Equality Impact Assessment

10.2 **Categories of access**

10.3 Internet Access for Service users – **Local Protocol**

10.4 **Internet Access passports**

10.5 Posters for display by Trust computer equipment – **Privacy**

Posters for display by Trust computer equipment – **Using Social Media Guidance**

10.1 – Equality Impact Assessment

Equality Analysis Screening Form
A word version of this document can be found on the HR support pages on Connect
http://connect/corporate/humanresources/managementsupport/Pages/default.aspx

Title of Proposal	Internet Access for Service User's (policy review)		
Person Completing this proposal	Kirsten Jones	**Role or title**	Chief AHP / Associate Director for Recovery, Experience, Spiritual Care & Physical Health
Division	SCOH	**Service Area**	Women's Secure Service & CAMHS inpatient
Date Started	27/08/24	**Date completed**	09/09/24

Main purpose and aims of the policy and how it fits in with the wider strategic aims and objectives of the organisation.

This policy is being reviewed in line with trust guidance and procedures surrounding the timely updates of current policies. This policy aims to facilitate access to the internet for service users and families within Trust ward settings to support recovery. Where risks exist, this access might be restricted on an individual basis with a clear rationale recorded and regular review times agreed.

Who will benefit from the policy?

Service users, families and carers, stakeholders within services.

Does the policy affect service users, employees or the wider community?
Add any data you have on the groups affected split by Protected characteristic in the boxes below. Highlight how you have used the data to reduce any noted inequalities going forward

This policy affects service users, carers and family. The Trust acknowledges the importance of internet access in everyday life in line with modern day human rights and aims to support access for service users, carers and visitors where it is safe to do this, and least restrictive practice can be utilized. The purpose of this policy is to outline procedures for ensuring that internet access is available for service users where appropriate, either using mobile devices and/or computing facilities provided by the Trust. This policy will support reducing inequalities by ensuring fair and equity access to the internet.

Does the policy significantly affect service delivery, business processes or policy?
How will these reduce inequality?

This policy does not significantly affect service delivery, business processes or policy.

Does it involve a significant commitment of resources?
How will these reduce inequality?

There may be a requirement for clinical areas to provide digital resources to support service users gain access to the internet in event of them not having access to a personal device. This requirement would reduce inequalities by offering fair and equitable access to the internet

Does the policy relate to an area where there are known inequalities? (e.g. seclusion, accessibility, recruitment & progression)

This policy supports reduction of inequalities across all service areas but clarifying acceptable standards for internet usage and availability of digital resources for all

Impacts on different Personal Protected Characteristics – *Helpful Questions:*

Does this proposal promote equality of opportunity? Yes provided access is provided equitably.	*Promote good community relations? This policy has the ability to increase*
Eliminate discrimination? Yes, as above it is important that access is available equally.	*Promote positive attitudes towards disabled people?*
Eliminate harassment?	*Consider more favourable treatment of disabled people?*
Eliminate victimisation?	*Promote involvement and consultation?*
	Protect and promote human rights?

Please click in the relevant impact box and include relevant data

Personal Protected Characteristic	No/Minimum Impact	Negative Impact	Positive Impact	Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.
Age	x		x	Due to the diversity of the age group of users it is intended for this policy to have a positive impact on all. The foundation principle of this policy is to improve digital literacy whilst receiving our services. for young people as this policy opens up ways to increase / maintain contact whilst in hospital. There may be not be an impact on people who are not familiar (perhaps older) / do not own smart phones or tablets.

				Use of risk assessment to limit access is individually applied and therefore should not have a different impact due to age.

Including children and people over 65
Is it easy for someone of any age to find out about your service or access your proposal?   Yes
Are you able to justify the legal or lawful reasons when your service excludes certain age groups? No age groups excluded.

Disability			x	The trust will make every attempt to provide reasonable adjustments to ensure equal access and its application. This policy will support integration and access with the wider on line community.

Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues
Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Yes
Are you making reasonable adjustment to meet the needs of the staff, service users, carers, and families? Yes

Gender	x			Policy is written to be used in a fair way across all genders including non binary.

This can include male and female or someone who has completed the gender reassignment process from one sex to another
Do you have flexible working arrangements for either sex? Yes
Is it easier for either men or women to access your proposal? Equal access

Marriage or Civil Partnerships	x			Policy is written to be used in a fair way across all relationships in some situations it can enhance relationship due to increased contact.

People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters
Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships? Yes

Pregnancy or Maternity	x			Policy is written to be used in a fair way across all relationships in some situations it can enhance relationship of parents and children due to increased contact.

This includes women having a baby and women just after they have had a baby
Does your service accommodate the needs of expectant and post natal mothers both as staff and service users? Yes
Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity? Yes

Race or Ethnicity			x	The policy seeks to be delivered to all equally however due to potential language barriers translated formats will be required and extra attention to be paid to ensure that access is equal.

Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees What training does staff have to respond to the cultural needs of different ethnic groups? Equality and diversity. What arrangements are in place to communicate with people who do not have English as a first language? Access to Interpreters as and when necessary.				
Religion or Belief			x	This might present increased opportunities for people to access faith activities.
Including humanists and non-believers Is there easy access to a prayer or quiet room to your service delivery area? Yes When organising events – Do you take necessary steps to make sure that spiritual requirements are met? Yes				
Sexual Orientation			x	This might present increased opportunities for people to access support related to sexual orientation such as online support groups and charities
Including gay men, lesbians and bisexual people Does your service use visual images that could be people from any background or are the images mainly heterosexual couples? Both Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea? Comfortable being out				
Transgender or Gender Reassignment			x	This might present increased opportunities for people to access supported related to transgender and gender reassignment such as online support groups, NHS websites and charities
This will include people who are in the process of or in a care pathway changing from one gender to another? Yes Have you considered the possible needs of transgender staff and service users in the development of your proposal or service? Yes				
Human Rights			x	Increased autonomy and increased access to family life
Affecting someone's right to Life, Dignity and Respect? No Caring for other people or protecting them from danger? The detention of an individual inadvertently or placing someone in a humiliating situation or position?				
If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998). No determined disproportionate impact.				
	Yes		**No**	

What do you consider the level of negative impact to be?	High Impact	Medium Impact	Low Impact	No Impact
				X

If the impact could be discriminatory in law, please contact the **Equality and Diversity Lead** immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required.

If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the **Equality and Diversity Lead** before proceeding.

If the proposal does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the **Equality and Diversity Lead.**

Action Planning:

How could you minimise or remove any negative impact identified even if this is of low significance?

Ensure that information is communicated effectively to all

How will any impact or planned actions be monitored and reviewed?

Service user experience and audit.

How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.

If an individual is to have a disability which impacts their ability to affectively use the means of internet access that is provided by the trust, then at a local level reasonable adjustments should be made to promote equal opportunity for these individuals by the necessary means.

Please save and keep one copy and then send a copy with a copy of the policy to the Senior Equality and Diversity Lead at **bsmhft.edi.queries@nhs.net** The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis

10.2   Categories of access

	User A	User B	User C	Skype Only
Adverts	Blocked	Blocked	Blocked	Blocked
Alcohol & Tobacco	Blocked	Blocked	Blocked	Blocked
Arts & Entertainment	allowed	allowed	allowed	Blocked
Auctions	Blocked	Blocked	Blocked	Blocked
Automotive	Blocked	Blocked	Blocked	Blocked
Business & Commercial	Blocked	Blocked	Blocked	Blocked
Computing & Internet	Blocked	Blocked	Blocked	Blocked
Dating	Blocked	Blocked	Blocked	Blocked
Drugs	Blocked	Blocked	Blocked	Blocked
Education	allowed	allowed	allowed	Blocked
Finance & Investment	allowed	Blocked	allowed	Blocked
Food & Drink	allowed	allowed	allowed	Blocked
Gambling	Blocked	Blocked	Blocked	Blocked
Gaming	Allowed	Blocked	Allowed	Blocked
Government	Blocked	Blocked	Blocked	Blocked
Hacking	Blocked	Blocked	Blocked	Blocked
Hate & Discrimination	Blocked	Blocked	Blocked	Blocked
Health	allowed	allowed	allowed	Blocked
Illegal	Blocked	Blocked	Blocked	Blocked
Image Sites	Blocked	Blocked	Blocked	Blocked
Instant Messaging	Blocked	Blocked	Blocked	Blocked
Internet Telephony	Blocked	Blocked	Blocked	Blocked
Lifestyle & Culture	allowed	allowed	allowed	Blocked
Military	Blocked	Blocked	Blocked	Blocked
News	allowed	allowed	allowed	Blocked
Newsgroups & Forums	Blocked	Blocked	Blocked	Blocked
Offensive & Tasteless	Blocked	Blocked	Blocked	Blocked
Peer To Peer	Blocked	Blocked	Blocked	Blocked
Pornography & Adult Material	Blocked	Blocked	Blocked	Blocked
Property & Real Estate	allowed	allowed	allowed	Blocked
Proxy Avoidance	Blocked	Blocked	Blocked	Blocked
Recreation & Hobbies	allowed	allowed	allowed	Blocked
Recruitment	allowed	allowed	allowed	Blocked
Reference	allowed	allowed	allowed	Blocked
Religion	allowed	allowed	allowed	Blocked
Search Engines	allowed	allowed	allowed	Blocked
Sex Education	Blocked	Blocked	Blocked	Blocked
Shopping	allowed	allowed	Blocked	Blocked
SMS & Mobile Telephony Services	Blocked	Blocked	Blocked	Blocked
Software Download	Blocked	Blocked	Blocked	Blocked
Sport	allowed	allowed	allowed	Blocked
Streaming Media & Media Downloads	Blocked	Blocked	Blocked	Blocked
Translation	allowed	allowed	allowed	Blocked
Travel	allowed	allowed	allowed	Blocked
Violence	Blocked	Blocked	Blocked	Blocked
Weapons	Blocked	Blocked	Blocked	Blocked
Webchat	Blocked	Blocked	Blocked	Blocked
Weblogs & Social Interaction	Blocked	Blocked	Blocked	Blocked
Webmail	allowed	Blocked	allowed	Blocked

10.3   Internet Access for Service Users Local Guidance template

<p align="center">**INTERNET ACCESS FOR SERVICE USERS
LOCAL PROTOCOL**</p>

<p align="center">*name of service*</p>

INTRODUCTION

BSMHT provides service user access to the Internet and other information technology to support educational, recreational and cultural needs.

This protocol clarifies the scope of use of information technology by service users at xxx and aims to minimise associated risks and ensure that computing facilities provided for service users have safeguards against misuse.

This protocol gives clear guidelines on the requirements for accessing the computers and internet and should be read in conjunction with the Trust's policy on Internet Access for Service Users.

AIMS

AVAILABILITY

PROCEDURE

SECURITY

Please add any other local security issues

DOS

DON'TS

For further information, please view the Internet Access for Service User internet pages on Connect;
http://connect/corporate/ICT/servicedelivery/Pages/SDSC/SDSC-INASU.aspx

10.4 Internet Access passport

Birmingham and Solihull NHS
Mental Health NHS Foundation Trust

INTERNET PASSPORT

This internet passport belongs to:

....

Topics that should not be accessed

Topic	Date added

A list of topics that I should not be accessing is also stored in my clinical documentation (Rio) under 'Internet Permissions'

Service User Internet Agreement

When using the internet, I agree to the following terms:

- The agreed access permissions and topics to be avoided will be written in my Internet Passport and date-stamped. Permissions agreed and declined will also be recorded in my clinical documentation (Rio).
- I will bring my Internet Passport to every internet session so that it can be checked by staff.
- Failure to bring my internet passport may result in my access being denied at that time.
- Any defacing of the passport, making it illegible or cast doubt on its validity may result in my access being denied at that time
- I will be supervised by staff during access to the internet at the level stated on the passport.
- I will not try to view content which my clinical team have identified and recorded on my passport
- I will maintain my own and others confidentiality
- I will not download software, material or data onto the hard drive.
- I will not view or use material, data or images that could cause harm, offense or harassment to another person.
- If a site is deemed inappropriate by supervising staff, I will shut it down when they ask me to.
- Staff can monitor the history of internet sites I visit.
- If staff have any concerns about my internet use, mental state, behaviour or attitude, access will be stopped until reviewed by the ward/clinical team.

I agree to comply with the rules above. I understand that if I do not, my access to the internet can be stopped.

Signature _____

Date _____

Access permissions

	Date granted
Internet browsing	
Online shopping	
Online banking	
Email	
Skype	
Education	
Other _____	

Supervision Level

	Date granted
1:1 (Intermittent)	
1:1 (constant)	
Group (2+)	

10.5 Posters for display by Trust computer equipment and in unit areas where visitors may be present - Posters referenced in this policy are available via the Trust's intranet or can be ordered through the Patient Experience Team. Display in inpatient areas is mandatory."

Birmingham and Solihull
Mental Health NHS Foundation Trust
NHS

TH!NK PRIVACY

Privacy:

Service users taking images/recordings of staff on camera phones or mobile devices

What should I do if a patient asks to record the consultation/session?

Increasingly people are making the use of mobile technology to record sessions. Whilst you have the right to privacy any decision should take into account the following:

1. The purpose for the request
2. Whether you feel that the information could be misused
3. Whether any other individual's privacy could be compromised
4. The impact on the conduct of the consultation/session e.g. could it make the discussion less open
5. The individual's rights/interests

- If you are happy for the recording to continue then you will need to set some rules around the recording such as the recording is for personal use only
- You may prefer to just have a sound recording and not have images taken
- If you are not comfortable with the recording taking place at all, you should inform the person and ask them to put the phone or other equipment away

What else do I need to consider?

The patient or service user may have valid reasons for asking to record the session and it could be seen as a right under the Disability Discrimination Act e.g. if the person has memory problems or difficulty hearing

What if the person makes a recording without consent?

Where it becomes apparent that someone has made a recording without consent, contact the Information Governance Team as we may need to send a notice asking them to delete all copies. If the recordings are put in the public domain it may be possible to get the site owner to remove them.

Recordings in public areas
Patients/service users should be advised that recordings are not permitted in wards, clinics or other public areas as it may impact on the confidentiality of other service users

Further Information
Contact the Information Governance Team:
Email:
InformationGovernance@bsmhft.nhs.uk

Version 1_00

Using Social Media Guidance

Whilst the Trust recognises the importance of social media as a means of engaging with stakeholders and partners, we are also aware that there are risks in terms of confidentiality and privacy which this guide should help you to avoid.

What do we mean by social media?

The term social media is used in this context to include all online applications which allow people to create and exchange content e.g. Facebook, Twitter, Blogs, Internet Forums and Lists, You Tube, Linkedin etc.

Key Principles

The IG Team supports the Trust initiative to get more members of staff to benefit from social media in a professional capacity. However, it is important to remember whether we are communicating verbally, in writing or electronically there are principles, guidelines and laws which protect the personal information of patients/service users and colleagues, which apply equally to our use of social media even where it is used in our private lives.

Individuals can be identified from images and descriptions as well as from personal identifiers

Privacy

Whether you are using social media in your private life or in your professional capacity you need to be aware that information which is posted online may be visible to others who are not the intended recipients. Information can be reposted and privacy settings frequently change. Once information has been posted it is often difficult to remove or permanently delete.

Top Tips for Using Social Media

1. Never share patient/service user identifiable information (even with other professionals in closed forums)
2. Do not discuss patient/service user care with the patient or their representative via social media
3. Keep your private and professional life separate, by referring patients or clients to other forms of communication if they contact you through your personal profile
4. Remember that you are accountable for anything you put online in the same way as if you published information through more traditional routes i.e. copyright, defamation etc. still apply
5. Respect the privacy of colleagues i.e. do not post pictures of colleagues or discuss them, other than in a social context with their knowledge and consent.
6. Do not post, share or comment on other posts which do not adhere to the Duty of Confidentiality or the Trust's values
7. Ensure use is consistent with relevant professional codes of conduct
8. Consider the impact of postings on the Trust's relationship with stakeholder organisations