.

STANDARD OPERATING PROCEDURE FORENSIC - PATIENT INTERNET AND MASS STORAGE DEVICES

Document Reference	SOP20-052
Version Number	2.0
Author/Lead **Job Title**	Adrian Deakin Project Security Lead
Instigated by: **Date Instigated:**	Security Committee
Date Last Reviewed:	6 March 2023
Date of Next Review:	March 2026
Consultation:	Security Committee
Ratified and Quality Checked by: **Date Ratified:**	Security Committee 6 March 2023
Name of Trust Strategy/Policy/Guidelines this SOP refers to:	

VALIDITY – All local SOPS should be accessed via the Trust intranet

CHANGE RECORD

Version	Date	Change details
1	*October 2023*	*Review, amendments to names, placed in new format.*
1.1	*June 2021*	*Clarification on low secure Wi-Fi access and mass storage devices.*
2.0	*March 2023*	*Reviewed. Change of SOP title and amalgamation of three SOPS (Mass Storage Devices, Skype and MS Teams and Patient Internet / Wi-Fi) into this one single SOP. Approved at Security Committee (6 March 2023).*

Contents

1. INTRODUCTION

In line with the NHS's national digital strategy, Humber Teaching NHS Foundation Trust offers open registration Wi-Fi in all in-patient units. Due to the complex profile of the patient group, and the risks posed, there is a need to manage this facility slightly differently in forensic in-patient units. This procedure has been developed to support service staff in optimising safe and appropriate internet and Wi-Fi access by that patient group.

Care Quality Commission (CQC) –
Access to Skype, MS Teams or internet chat rooms will be informed by the patient's ability to make safe and appropriate use of the internet for such purposes within their recovery journey. Access to internet chat rooms and similar technology is an everyday activity for most members of the population. A recovery approach suggests that access to such technology should be possible for all patients as soon as it becomes appropriate with regard to their treatment pathway and any risk management strategies.

It is important to find a balance between:

- the needs of patients to maintain communications and contact with family and friends; and
- the need to protect people against the misuse of advanced technology
- providing a therapeutic environment
- protecting the rights of individuals
- protecting people from abuse
- promoting recovery
- protecting confidentiality
- promoting acceptable standards of behaviour
- Management of risk

Restrictive Practice
This procedure does, to a certain extent, constitute a blanket restriction to patient access to the internet or public Wi-Fi. Access is granted on an individually assessed basis by the MDT, within the parameters regarding patients on low and medium secure wards, as described in the following paragraph.

Patients on low secure wards can be considered for unsupervised use of Wi-Fi within the unit. Patients on medium secure wards cannot be considered for unsupervised use of Wi-Fi within the unit – for that patient group it is reasonable and proportionate that any access to the internet will require a degree of supervision / support as part of service security measures. Why a difference between Low and Medium? There is an inherent assumption that all patients in MS pose more risk than all patients in LS for all things. Is this true?

This variation in level of restriction is judged to be both necessary and proportionate. Patients admitted to medium secure services present a serious risk of harm to others (NHSE, 2018) and certain blanket restrictions are acknowledged to be necessary in order to maintain the overall security of the service and to manage high levels of risk to other patients, staff and members of the public (NHSE, 2018).

Internet access is regularly reviewed and any rationale for restriction is recorded.

There is a degree of restriction in the use of finite resources of equipment (laptops, access to education room), availability of staff, etc. and the service will endeavour to provide fair and equitable access along with access to mass storage devices. Secure Services strives to allow access to mass storage devices to all patients following an individual risk assessment. The purpose of this standard operating procedure is to identify a process that enables the maintenance of the security of the service whilst being least restrictive in accessing technology and devices.

2. SCOPE

This procedure applies to all patients detained at the Humber Centre, Pineview and South West Lodge. It informs all staff in accordance with their duties and responsibilities to adhere to Information Governance and Confidentiality policies, the process of managing the security impact of patients' access to the internet and use of mass storage devices.

This procedure does not apply to staff, whose use of the internet is addressed by Trust policy - Electronic Communications and Acceptable Use of the Internet Policy

3. DUTIES AND RESPONSIBILITIES

The Security Committee will monitor and review this procedure, reporting to the Clinical Network. All staff within the service will be aware of this procedure and work within it.

MDTs will consider and review the nature and degree of internet and for Low secure only Wi-Fi access for each patient at least every three months.

Identified staff will be registered with the IT Department to create, manage and discontinue Wi-Fi accounts for patients. The list of registered staff will be available from reception – displayed on the notice board.

These staff will access the required site at; https://sponsor.humber.nhs.uk, using their Trust IT log- in user name and password.

4. PROCEDURES

4.1. Equipment

Each ward will retain and maintain a laptop exclusively for patient use in accessing the internet. To be signed out and stored securely when not in use. Individual wards may also consider installation of a PC in an access-controllable area of the ward.

Cameras and microphones on such laptops / PCs will be disabled. No Mass storage devices to be connected to trust Laptops/PC. The education room will continue to provide access to Skype.

- One computer in the education room at the Humber Centre will have a webcam (including microphone) and speakers. This computer will be used for all Skype and Microsoft Teams contact. Furthermore, there will be a 'slave' monitor to enable staff to discretely monitor the contact, where deemed necessary.
- One computer at Pine View will be similarly equipped, though there will be no need for a 'slave' monitor
- A tablet is stored in the reception control room and wards have two stored in the ward office for use in visitor's room for video communication.

Service users will need a memory stick or other storage device if they wish to save any work they do on a computer. No data should be saved to the hard drive of the Trust computers.

Service users may only use memory sticks purchased by the service on trust computers. USB storage devices purchased by patients may present a security risk.

4.2. Risk Assessment

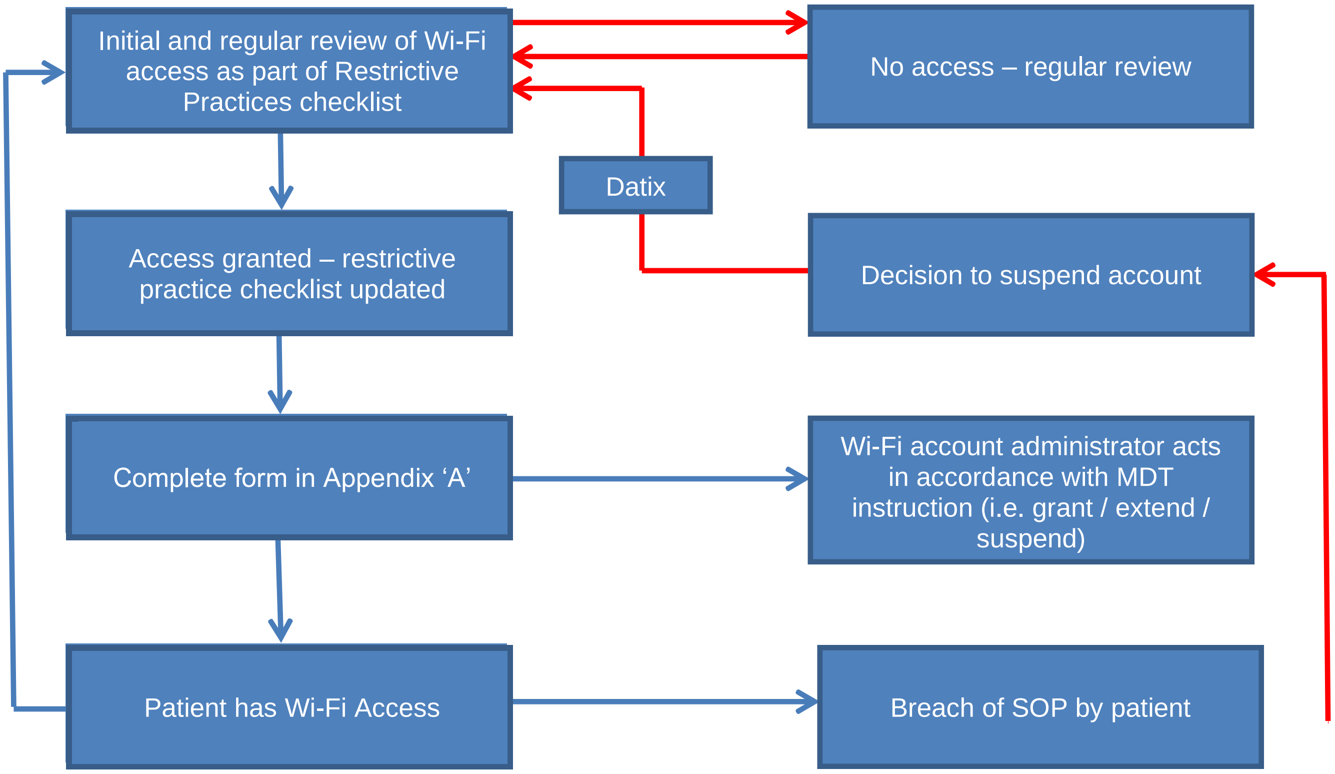
The nature and degree of internet access and use of mass storage devices will be included in the Restrictive Practices Checklist for all patients.

Clinical teams may grant one of four levels of access;

A. No access to the internet.
B. **Supervised** access to the internet via PCs in the education room or on the ward, using laptops / PCs provided by the service.
C. **Unsupervised** access to the internet via PCs in the education room or on the ward, using laptops / PCs provided by the service.
D. Access to Wi-Fi on own device(s). Available to patients on low secure wards only.

A – Risks have been identified which preclude access to the internet. The patient will, therefore, not have access to the internet under any circumstance.
B – Internet access requires the presence, support and supervision of staff. Staff will maintain an awareness of the sites being viewed, without observing the content of e-mails, posts social networking sites, or knowledge of passwords, PIN numbers, log in details, etc. (see 5.3 and 5.4 below). Risk assessment must identify any specific sites or categories of sites / content that the patient may not access.
C – Staff are facilitating access to equipment (by signing out ward laptops / tablets) or to the education room (and acting as escort) but are not monitoring in any way the sites visited, but are ensure that no mass storage device is being connected to a computer that is connected to the internet.
D – Patients may access Wi-Fi on personal devices within their bed space only, which may, themselves, be managed by a care plan. There is no monitoring of sites visited. **Available to patients on low secure wards only.**

4.3. Creation and Management of Patient Wi-Fi Account


Initial and regular review of Wi-Fi access as part of Restrictive Practices checklist
No access – regular review
Datix
Access granted – restrictive practice checklist updated
Decision to suspend account
Complete form in Appendix 'A'
Wi-Fi account administrator acts in accordance with MDT instruction (i.e. grant / extend / suspend)
Patient has Wi-Fi Access
Breach of SOP by patient

4.4. Staff Support of Patients in Accessing the Internet

Supported access does not exclusively involve policing sites accessed. It can involve enabling patients to access the internet in meaningful ways that support their recovery, and do not expose them or others to risk of harm, exploitation, abuse, etc.

A patient who has mental capacity, may reasonably request staff support in composing e-mails or similar, in much the same way as support in writing a letter may be requested. If the staff member is in any way uncertain, then they should seek guidance before doing so. If support is agreed, it must not go so far as to include knowledge of passwords, PIN numbers, etc.

Staff may advise / remind the patient about any restrictions included in the Restrictive Practices Checklist. This will be individually risk assessed by the relevant MDT and documented in the Restrictive Practice Plan. This will include the use of MS Teams and Skype:

- Patient and care co-ordinator will discuss the option to use Skype and Microsoft Teams for remote contact
- The patient's request must be supported by the MDT (and a supporting entry made in the restrictive practice plan – this will stipulate any limits / conditions)
- All Skype and Microsoft Teams use will be 'booked' in advance in the same way as a face-to-face visit – this will ensure that staff and resources are available
- Staff will support patients in establishing a Skype and/ or Microsoft Teams account **but will not become aware of the patient's personal and confidential password**
- Prior to the commencement of Skype and Microsoft Teams use, there will be a discussion with the patient to ensure that any necessary boundaries / limits etc. are acknowledged, and that the contact will be terminated in the event of any breach of set boundaries

4.5. Staff / Team Intervention and Support

This can include:

- Advising the patient that the site (about to be) visited is not one supported by the MDT
- Immediately disabling internet access in the education room using the switches installed
- Suspending the patient's account, whether immediately or at MDT review
- Staff supporting a Skype contact will be familiar with, and competent in, the use of Skype and Microsoft Teams and its associated equipment
- Skype and Microsoft Teams will be used to enhance contact with friends, families and carers – not as a substitute for face-to-face contact when such contact is possible
- A Skype and Microsoft Teams contact will be managed in the same way as a visit – this will involve room booking via reception
- Escorting staff will remain out of camera shot as much as possible but may need to intervene if they became aware of any inappropriate interactions or other issues of concern, as they would in a face to face visit. They may also need to support the patient with the use of the IT equipment.

Any intervention which limits / suspends access may cause irritation to the patient and summoning additional support may be considered.

A Datix must be completed.

Software is in use that will limit access to certain websites. Access (attempted or actual) to sites of the following nature without MDT approval will immediately prompt the discontinuation of the session and review of continued internet access:

- Sites showing violent or criminal activity
- Pornography
- Websites promoting violence, abuse or hate
- Sites offering information about other patients (though this may be in the public domain, it may add to risk within the clinical environment)

- Gambling (unless already agreed and planned by the MDT)
- Purchasing items that contravene the existing contraband list

4.6. Mass storage devices

4.6.1 Memory Sticks

Prior to issue of a memory stick, service users will sign the Safe Use of a Memory Stick Agreement (Appendix B)

Memory sticks will be labelled with the service user's name, issued by the ward and stored in the security cupboard. As restricted items, they are not permitted in service user's bedrooms.

Memory sticks are signed in and out with each use. The checking of memory sticks is part of the ward's security checks.

Service users may choose to password protect files on their memory stick. Should a service user lose their memory stick this may help to ensure that personal information remains private.

Memory sticks will be subject to routine checks of their contents, including password protected files. Checks may additionally be carried out where there have been concerns about increased risk, for example where there have been unconfirmed reports that inappropriate files are on the memory stick, on transfer to another ward, or if a service user is AWOL and staff feel there may be useful information. Frequency to be document in the patient safety plan.

Where possible, search checks will take place in the presence of the service user. For password protected files, the service user should enter the password to enable staff to view the document. Refusal to do so will lead to a response that the material is unsuitable and may result in the memory stick being removed and the file being deleted or access to mass storage devices removed.

4.6.2 Service User owned personal computers (laptop and tablets without cameras)

Subject to individual risk assessment and agreement by the care team, service users may be allowed access to their own computers and tablets.

A care plan and separate computer use agreement must be in place for this to be accessed on the ward.

Service users must not access the internet on their personal computers or tablets on the ward or in bedrooms.

Service user owned computers may only be used in bedrooms if the internet access has been disabled.

Access to personal computers during escorted and unescorted S17 is risk assessed and managed on an individual basis by the care team. However, if the patient chooses to take the device outside of the perimeter, then they cannot access it inside the perimeter

Staff will make random checks whilst a service user is using their own computer, if they have unsupervised access. If, at any time there are any concerns about a breach of the agreement, access will be suspended pending review by the care team.

Personal computers or tablets are stored in the ward security cupboard.

Personal computers must be switched off when they are being stored or charged.

Routine memory stick / MP3 player search record is to be completed each time a routine check is carried out, using the trust search documentation.

Routine checks will also take place on non-networked computers to minimise the risk of viruses.

Software that is held on CD, DVD or other media should be checked by ward staff. If approved, this must be installed by the Trust IT department.

Service users will be offered the option to take their memory stick with them when they leave the service.

4.6.3 Handheld games/games consoles

Trust owned games consoles are available for use by service users in communal areas of the wards.

Access to own games consoles in private bedrooms is subject to individual risk assessment.

Access to 18 rated material is subject to agreement of the care team (see SOP).

As part of the ward security checks, all devices will be subject to routine checks for medium secure and random searches for Low secure.

Only Devices that don’t require access to the internet are permitted in the secure perimeter

In the event of concern about a risk of breach of the agreement and / or concerns about reduced engagement, access may be suspended pending discussion by the care team.

Low secure patients with WiFi access may have access devices that require internet access following MDT approval.

4.6.4 Dongles (a small device which attaches to a computer, TV or other device, in order to enable access to wireless broadband or additional functions)

Patient own Dongles are not permitted at the secure service. However, staff may use these as part of a supervised activity

4.6.5 MP3/4 Devices (a small portable device capable of storing files downloaded from the internet or transferred by CD)

Access to an MP3/4 player is subject to individual risk assessment, agreement by the care team and the service user signing an agreement. Any device that has the ability to record sound / images is not permitted within the secure perimeter.

Access to MP3 players varies on each ward and there may be local restrictions, documented in the Ward Safety and Security profile.

It is not permitted to record sound / images on devices. MP3/4 players will be subject to random checks by staff and on suspicion of a breach of the agreement.

In the event of a breach of the agreement, access to devices will be suspended prior to review by the care team.

No access to memory chips other than SIM cards for mobile phones, as these items can be easily go in and out of the secure perimeter containing illegal or inappropriate material, and then shared around the service which put the integrity of the security of the service at risk.

4.6.6 Charging MP3/4 players or other devices

Many devices, such as iPods or other MP3 players recharge their internal battery by plugging them into a computer using some form of USB cable. These are not to be plugged into a networked computer. These cables are stored as a security item.

Service users with USB charged devices are advised to discuss buying a USB plug with their ward manager. These plugs enable MP3 players to be charged from wall sockets. Depending on the security profile of the ward the charger may be used in the service user's own bedroom or in the ward office. Managed as a controlled item

4.6.7 Transferring Music /Video to USB storage device

Music CDs can quickly and easily be transferred into a computer format that can be transferred to generic MP3 players.

An MP3 player connected to a computer by USB cable is essentially an external hard drive, similar to the USB memory sticks.

MP3 players could be used to store inappropriate documents / pictures etc. As a result direct supervision is required for this activity.

The MP3 player has the potential to carry computer viruses. The computers provided for patients by the Trust are not networked and separate from staff computers which means that under direct supervision it is possible to use these computers to do this in the following circumstances;

The device cannot be connected to a computer with internet access.

The music is copied on the service users own MP3 player (copyright protection)

The music files created during this process are deleted from the Trust computer at the end of the session. It is permissible for service users to also transfer these files to their own hospital purchased, USB storage device either due to data storage limitations of their MP3 player, or as a backup.

A computer without internet access will be available for patients in the education room, and some ward identified on the wards, WSSP (ward Safety and Security Profile)

4.6.8 Installing Software and downloading internet files

Service users are not permitted to download or install software

Any software required must be agreed by the patients MDT, and then passed by the security group, who will ask IT to add the software to the patient computer in the education room,

Service users may download material approved by supervising staff onto their own memory stick. The patient can only access this material in the education room.

Material should not be downloaded onto the computer hard drive.

No files tagged '.exe.' should be downloaded as these are for installing programmes.

No other mass storage device can be connected to the internet, unless the patient has been granted open access to the Wi-Fi system, low secure only.

4.7. Search

There may be intelligence that a search of the equipment used to access the internet/Wi-Fi or storage devices may be required. Staff will be guided by the Patient Search Policy and the Search SOP.

If a search is required the Security Team for the Humber Centre should be contacted to arrange a suitably mandated and qualified person to undertake. Any search will be recorded as a Datix as per the Trust policy.

If illegal images or data files are found as part of a search, all mass storage devices on the ward that patients have had access to, must be seized and stored in evidence bags, and are to be search following advice from the police. Searches of mass stored devices are to be carried out by trained staff only. Staff conducting search must be aware that they may need to provide a statement to police if something is found.

If there is the suspicion that the device contains illegal images, then the device is to be sealed in an evidence bag and given to the police for investigation. So that the police evidence trail isn't breached or compromised. No search to be carried out by trust staff.

There must be two staff present at all times when conducting a search of storage devices.

If illegal images are found on a computer whilst conducting a search, then the search is to be stopped immediately, the device sealed in evidence bag and police contacted. The staff conducting the search must complete a Datix, and individual supervision given to provide support. Consideration must be given to utilising the occupation health service at this point.

If the patient wishes to be present during the search the Education room or activity room off the ward to be used to conduct the search.

All searched of devices will be conducted using a none networked device.

Patients within South West Lodge are individual risk assessed for which mass storage devices they can access, there are no limitations to the devices they can access or the devices capabilities imposed by the service.

Access is granted based on the following guidance, that the device doesn't pose a risk to the integrity of security for the service, devices aren't shared with other patients, and that the patient doesn't bring the devices into Pineview or Humber Centre.

In the event that a patient is transferred from South West Lodge into another part of the inpatient service, then all devices are to be search before access to the devices is granted.
All searches of devices are to be conducted at random as documented in the ward safety and security profile.

5. IMPLEMENTATION

All new staff will be required to read the service procedures as part of their service security induction and security refresher.

6. MONITORING AND AUDIT

This procedure will be monitored by the Security Committee.

7. REFERENCES

- Care Quality Commission (2016) Brief guide: the use of 'blanket restrictions' in mental health wards
- Department of Health (2015) Mental Health Act 1983: Code of Practice
- NHS England (2018) Service Specifications for Adult Medium Secure Services
- Department of Health (2009) Using Mobile Phones in NHS Hospitals
- Department of Health (1983) Mental Health Code of Practice
- The Human Rights Act (1998) Office of Public Sector Information (OPSI)

Appendix A: Wi-Fi Account Record / Action Log

Humber Centre for Forensic Psychiatry Wi-Fi Account Record / Action Log

Name	
NHS Number	
DoB	
Ward	

Initial agreement for the patient to register for Wi-Fi access was taken on; _______________

Review of access

	Date	**Action required** **(Renew / Discontinue)**	**Sign & print (staff)**	**Date actioned**	**Sign & print (staff)**
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
3 month review					

To maintain access, this form must be submitted to any of the staff named below;
Dave King, Andy Lucas, Judi Cole, Rachel Boulton, David Farnsworth, Andrea Lord, Zoe Moon, Kay Appleyard

Each account renewal will automatically lapse after 14 days. Failure to action this sheet within that time will result in loss of Wi-Fi access.

Appendix B: Memory Stick Consent Form

Memory stick consent form

Patient name:______________________________.

Date:____________.

I agree that the encrypted memory stick I have received will be given back at the end of the internet session, will be held in the office and will be used under supervision only.

I agree that the memory stick is the property of Humber Teaching NHS Foundation Trust and will be handed back when I leave hospital.

Password:________________________.

I agree that it will be subject to inspection at any time.

Signed:_________________________.