PATIENTS' USE OF COMPUTERS AND ACCESS to the INTERNET in SECURE SERVICES PROTOCOL

POLICY NUMBER:	**SSOP 32**
AUTHOR:	**Secure Services Policies & Procedures Group**
IMPLEMENTATION DATE:	**November 2010**
AMENDMENT DATE(S)	**07/08/2012, 25/11/16, 14/03/19, 30/05/2019, 24/03/2022**
LAST REVIEW DATE:	**October 2013, 03/12/2013, 06/11/2014, April 2018; July 2021, July 2024**
NEXT REVIEW DATE:	**July 2027**
APPROVAL BY SERVICE MANAGEMENT TEAM:	**13/01/2014, 10/11/2014, 01/06/2018. Approved by SSMG on October 2024**

The Director responsible for monitoring and reviewing this protocol is:

The Director of Specialist Services

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PROTOCOL for PATIENTS' USE of COMPUTERS and ACCESS to the INTERNET within SECURE SERVICES – SSOP 32

CONTENTS	
Title	**Section No.**

SCOPE

Services	Applicable	Comments
Essex and Bedfordshire	✓	

PROTOCOL for PATIENTS' USE of COMPUTERS and ACCESS To the INTERNET within SECURE SERVICES

1.0 INTRODUCTION

1.1 Skills in using information technology are an important part of modern life with many day to day activities being simplified through the use of the internet for activities such as email and instant messaging, searching for information, banking and shopping. In preparing our patients for a return to the community it can be argued that teaching them skills in how to use the internet is an important part of their rehabilitation.

1.2 This document aims to set out a system for the safe, secure and legal use of internet facilities for use with service users both within the unit and in the community.

2.0 OBJECTIVES

2.1 Due to the risks associated with safely managing patient access to the internet, patients can access the internet in the IT Room (Therapies Suite) in Robin Pinto and Brockfield House. At Edward House and Wood Lea Clinic, there will be designated areas for safe management of patients' access to the internet.

- At present, Aurora Ward, Forest Ward, Causeway, Fuji and Dune Ward at Brockfield House have internet provision on a computer designated for patient use; this is located in the communal area of the wards. Alpine Ward and Lagoon Ward do not have internet access for patients due to connectivity costings and cabling issues, however patients on those wards subject to leave status will have access to a PC with supervision in the OT Therapy areas. Edward House, Robin Pinto Unit and Wood Lea Clinic have internet provision in their respective Therapy rooms. All Units in Secure Services have an IPad that can connect to pre- programmed sites for specific purposes only (e.g. access to video- conferencing with professionals). All accessible sites are pre-programmed into the each IPad by the IT department.
- Access to the internet on the ward PCs will follow similar guidelines as highlighted in Section 7.0 of this policy.

2.2 Patients may access the internet in the community on Section 17 leave as part of their rehabilitation with the agreement of their multidisciplinary team.

2.3 The guidelines below will outline how patient access to the internet in both of these circumstances will be safely managed and the safeguards to be used to manage potential risks

2.4 It is the responsibility any supervising staff member to be familiar with:

- SSOP 32 - The Secure services policy and procedure on Patient

access to the internet
- SSOP 8 - TV and Video Entertainment amenities for Secure Service Patients.

3.0 REVIEW AND MONITORING

3.1 This protocol will be reviewed periodically and amended, as necessary, by the Secure Services Policies and Procedures Group.

3.2 Periodically the patients' multidisciplinary team should review patients' access to the internet whilst on leave and ensure it is being used appropriately.

4.0 REFERENCE TO OTHER TRUST POLICIES/PROCEDURES

4.1 SSOP 32 - Patient Access to the Internet

4.2 SSOP 8 - TV and Video Entertainment amenities for Secure Service Patients.

4.3 Acceptable Use of Internet - pamphlet for Patients (SSOP 32, Appendix 1)

4.4 Access to Video-Conferencing in Secure Services (SSOP 32, Appendix 2)

4.5 Internet Use Contract (SSOP 32, Appendix 3)

4.6 SSOP 37, section 3.0 (prohibited items).

4.7 SSOP35 Use of Mobile Phones within secure Services

5.0 DEFINITIONS

5.1 Trust internet facilities are classified as the computer services and online facilities including intranet, email and worldwide web provided by the EPUT server and supported and managed by the Trust Information Technology (IT) department.

6.0 RESPONSIBILITIES

6.1 This policy must be read and observed by any member of staff who is to supervise patients accessing the internet.

6.2 All staff supervising patient internet access have a responsibility to monitor patient usage and intervene if there is a breach of the policy. They have a responsibility to report any breaches of the policy to their manager and the patient's multidisciplinary team (MDT) as well to record any such breaches in the patient's electronic record.

6.3 It is the responsibility of the patient's clinical team to risk assess whether they should be permitted access to the internet while on escorted Section 17 leave. Once agreed they have an ongoing responsibility to keep track of the patient's use of the internet and its relevance to their rehabilitation and act if they feel a breach has occurred or is likely.

6.4 The Policy and Procedures group is responsible for monitoring and reviewing this policy annually.

7.0 GUIDELINES FOR PATIENTS USING THE INTERNET in the SECURE SERVICES

7.1 Patients may be allowed to use the internet provided they have MDT approval and are supervised by staff at all times in the Therapy areas, whilst accessing the internet. Where the patient internet is available on the ward PC, this will be in the communal lounge or some other easily visible area on wards and as such visible to staff at all time. When the patient signs a contract for access to the internet, the MDT will decide whether or not their use should be supervised or whether it can be unsupervised. This will be reviewed periodically.

7.2 Use of the internet for patients should always be based on therapeutic outcomes such as learning skills, accessing education/training, maintaining contact with family/ significant others, and accessing clinical sessions with professionals. Therefore, patients are permitted to use the hospital internet for:

1. Browsing authorised websites including banking and shopping websites

2. Accessing Trust-approved video-conferencing portals to attend virtual family visits and/or remote clinical sessions with professionals (e.g.AccuRx).

3. Accessing personal email accounts (under supervision). Level of supervision will be reviewed time to time by MDT. IT access of ward will be supervised by escorting ward staff.

7.3 Patients will not be able to download or store any material to the hard-drive (C:\) of ward computers as such access has been disabled by the IT department. Patients must **not** be provided with individual windows logins to access the ward computer as this will create space on the drive that would enable patients to store inappropriate material.

7.4 Access to or the use of social media such as Facebook or dating websites/apps (e.g.Twitter, Snapchat, Instagram etc) will not be permitted whilst accessing the internet on Trust computers. Nursing staff will ensure fair and equitable access to all patients. Use of the internet by patients to purchase items must be approved first by the MDT and should be for specific items. The green form must be used in this instance.

7.5 Staff supervising patients using the internet must pay close attention to their usage and if a patient is seen to use the internet inappropriately then this must be documented and reported to patients' MDT who will review the patient's Internet contract.

7.6 Prior to accessing the internet, all patients must request access using the Internet Use Contract' (SSOP 32, Appendix 3). The respective MDT will consider this request and agree on whether the patient is allowed to have access to the internet. Patients should also be given a copy of Acceptable Use of the Internet - Pamphlet for Patients' (SSOP 32, Appendix 1). Patients must be encouraged to be aware of the possible risks attached to some on-line activities, including: broadcasting personal or private information over the network, making on-line financial transactions, being involved in or victim of cyber bullying, etc.

7.7 Use of USB Memory Sticks

7.8 Patients will be issued with Trust approved and encrypted USB sticks to store appropriate information downloaded from the internet during supervised access to the internet within the Unit. USB sticks are issued to patients following MDT approval and are for personal use only; they must not be shared between patients. USB sticks are considered a restricted item and must not be removed from the hospital under any circumstances (e.g. during Section 17 leave). As such, when not being used by patients, all USB sticks must be stored securely by staff (e.g. in the nursing station at Brockfield House; in lockers at Edward House, Robin Pinto and Wood Lea) who must sign them in/out for each use. Patients will only be allowed to take their personal USB sticks off the ward to use them in the IT suite under supervision. On these occasions the USB stick must be immediately be returned to their secure location at the end of their IT session.

7.9 USB sticks remain the property of the Trust and, whilst staff review of USB contents will not occur routinely, patients must agree to the MDT reviewing their content where this is indicated due to concerns around risk. Patients may discuss with staff who at their discretion will allow a reasonable amount of information to be printed from the computer.

7.10 The following are the locations where internet can be accessed by patients within EPUT secure services:

Brockfield House	IT Room, Therapies Suite, Ward PC, (where available)
Edward House	Therapies Suite; Ward PC
Robin Pinto Unit	Therapies Room, Ward PC
Wood Lea Clinic	Therapies Room; Ward PC

The IT/ Education room in Brockfield House may be used for the above purposes between 09.30 – 19.30 hours. The room must be booked in advance by contacting the administrator. Therapy and Educational programmes in the IT room will take precedence to any individual internet use requests. The use of the internet in the other units must be with the permission and supervision of nursing or occupational therapy staff. Where a patient has a planned therapy or OT activity session they will normally not be expected to use this time period for using the internet on the ward PC.

7.11 Where a patient has approval for home visits but has difficulty visiting the family due to limitations such as distance, the MDT may approve virtual visits by the use of video calling facilities such as Microsoft Teams or AccuRx programmes to contact family/ significant others. All protocols to do with facilitating home visit requests will have to be followed by the MDT before approving such requests (ID checks, supervision during the visit etc.).

7.12 The following are **not** permitted at any time when accessing the internet:

- Viewing of pornography or graphic violence
- Accessing of social networking web-sites whilst in the hospital
- Accessing dating sites such as Tinder and Bumble
- Downloading illegal music, DVDs, software or other files
- Playing violently or sexually graphic games of a certificate 18 rating
- Sending threatening, offensive, intimidating or abusive messages
- Making contact with a victim or a victim's relatives
- Sharing information about other patients or any other breaches of confidentiality or security
- Participating in online betting or gambling
- Ordering of drugs or alcohol (or other items prohibited within secure services).

7.13 The internet network at Brockfield House is managed by a 'parental controls' system to restrict access to most domains that host the above unauthorised materials; these controls are operated through the IT Department using the 'Open DNS' platform. Authorised users, such as Unit Coordinators, have access to the parental controls system.

7.14 The above list is not exhaustive and there may be other ways that patients can misuse the internet that are not mentioned here. Staff should use their discretion if they feel a patient is using the internet inappropriately and intervene by either stopping the patient misuse of the internet or end the session and return to the ward.

7.15 Before patients are permitted to use Microsoft Teams or AccuRx for appropriate virtual visiting or for clinical purposes, patients will need to have read and understood Appendix 2 of this policy 'Access to Video-Conferencing in Secure Services' and have MDT approval by completing Appendix 3 of this policy – 'Secure Services Internet Use Contract'.

7.16 Microsoft Teams or AccuRx conversations are permitted only between the patient and an agreed person. No one else will be permitted to join in the conversation. Patients are encouraged to be mindful of their conversations as others may be listening in to the patient's conversation at the receiving end.

7.17 Whilst using Microsoft Teams or AccuRx it is recommended that other patients are not present in the IT room/ designated area where a patient is using Microsoft Teams or AccuRx for reasons of privacy and confidentiality.

7.18 All Microsoft Teams or AccuRx calls must be supervised by a member of staff.

8.0 PATIENT ACCESSING THE INTERNET WHILE ON SECTION 17 LEAVE

8.1 Patients with unescorted area leave are permitted to access the internet while out in the community unless their multidisciplinary team (MDT) has placed specific restrictions upon the Section 17 conditions that the patient should not access the internet.

8.2 Patients with escorted area leave must have documented MDT approval in their clinical notes to use the internet whilst on leave under the supervision of an escorting staff member. The MDT must feel that any risks can be safely managed and that accessing the internet serves a therapeutic benefit either through development of skills or through engagement in a meaningful activity.

8.3 If the MDT approves a patient to access the internet while on leave, the patient will be given a pamphlet outlining what is deemed appropriate use and what will be considered an abuse of the privilege (Appendix 1)

8.4 Patients will be permitted to use search engines to research information, set up email accounts (their usage of which will be monitored by escorting staff), play games of certificate 15 and below, and other skills that may be taught through an IT skills course.

8.5 When using computers/ internet outside the unit, patients saving any information onto personal memory sticks or external drives must surrender these to staff on return to the secure unit. It is the responsibility of the escorting staff to ensure they obtain these items from the patient before they return onto the ward. This is in compliance with the Patient Amenities (TV & Video) Policy SSOP 8. All such items will be securely stored in the patient's restricted items box. The patient will be permitted to have access to them when they go on leave again. Under no circumstances should Trust-issued USB sticks for use within the hospital be taken out of the Unit.

9.0 GUIDELINES PATIENTS USING PCs AND WARD LAPTOPS WITHIN THE SECURE SERVICES

9.1 Every ward within the secure services should have access to at least one personal computer (PC) in the communal areas of the ward. Using any device to connect the PC to an internet network (other than the network provided by EPUT for patient use) e.g. using a dongle, mobile phone etc. is not allowed. Patients can plug in an approved MP3 (using detachable USB) in order to charge the battery or copy songs from a music CD. Patients will also be permitted to attach their Trust-provided encrypted USB stick to the laptop when using the laptop in the communal area of the ward or in their bedrooms; no other form of external storage device is permitted.

9.2 It is recognised that there will be occasions when a patient would like to have access to a laptop for therapeutic purposes - such as doing course work (for educational purposes) or writing personal letters to family/solicitor/friends. To accommodate this and provided there is documented multi-disciplinary (MDT) approval in place, patients can have access to a laptop provided by EPUT, for

short periods (up to a maximum two hours per day), to work from the privacy of their rooms or in a therapy area. This can be undertaken with or without supervision by staff based on the risk assessment and MDT approval. The laptop would not be permitted to be connected to the intranet.

9.3 All laptops/PCs for such patient access will have had any confidential / third party data removed from all drives and will have been disabled for internet access. Ward PCs will have been approved by the IT department as fit for use by patients and access to the hard-drive (C:\) will be disabled. It will be the responsibility of the Charge Nurse / Ward sister to ensure that no other laptops / PCs are accessible to patients in accordance with protocol SSOP 37, section 3.0 (prohibited items). .

9.4 No data of a personal nature can be saved on the laptop; nursing staff can check the laptop as required to ensure personal data has not been stored (access to the hard-drive is disabled) However, patients are permitted to store information on their Trust-approved and encrypted USB stick (see 7.7 above) . Completed work may be printed with permission of the staff.

9.5 Patients who have been issued with a trust approved and encrypted USB stick will be able to take these to their therapeutic sessions in the education room. Nursing staff are responsible for ensuring they are returned to the ward as per section 7.7 above.

9.6 Patients within the secure units are not permitted to keep personal laptops/ PCs / Tablets / Smartphones or any similar device that can connect to the Internet.

9.7 However, provided a patient has prior agreement from their MDT, a patient may have permission to access the Internet using their own smart mobile phone during their Section 17 leave (e.g. in a library, while visiting their family home or wherever there is a Wi-Fi connection) or, with certain conditions, whilst on unescorted perimeter leave (see SSOP35 for further guidance).

10.0 PROCEDURE FOR ASSESSING AND RESPONDING TO THE POTENTIAL FUNCTIONS OF TECHNOLOGICAL DEVICES

10.1 On the following pages please find a table of current popular technology along with the perceived risk and recommended access levels for patients (both in patient's bedrooms and in communal areas on the ward) and proposed risk management strategies where appropriate.

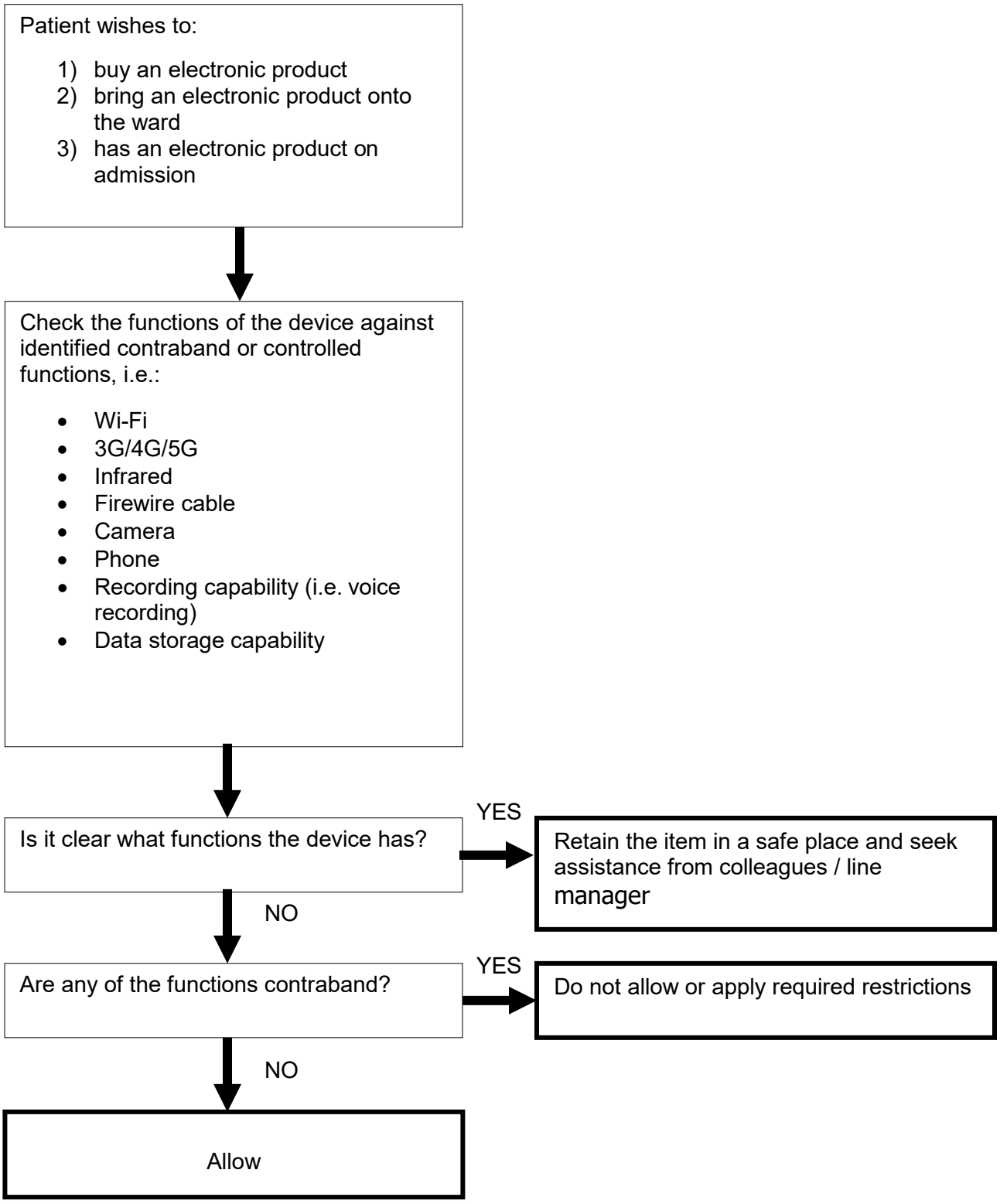
Device	Patient's Access to Technological Devices:		Additional Notes
	1) In patients' rooms (as a patient's personal possession)	**2) In communal areas on the ward** (as a device belonging to the ward/service)	
MP3 Player (eg. iPod)	MP3 Players with a screen that can display images are not allowed (for example an iPod would not be allowed) MP3 players with a screen that can only display text, are allowed.	Same as for patient's rooms.	MP3 Players with a USB / Fire-Wire socket and detachable cable are allowed as long as the cable is kept in storage and not in the patient's bedroom. Cable can only be used under supervision. Patients can purchase a plug charging adaptor so that they don't need to connect the MP3 with a computer to charge the device.
Trust approved and encrypted Memory sticks	Allowed when used with modified ward laptop that does not connect to the internet	Allowed under supervision due to ward PC connecting to the internet	This applies to Trust-issued encrypted USB sticks only subject to MDT approval. They must not be removed from the Hospital under any circumstances (see section 7.7 above)
Personal Memory sticks or personal memory cards	Not allowed	Not allowed.	This includes USB drives, USB sticks, USB "pens", flash drives, and MP3 players or other devices that have integrated USB. Only Trust approved encrypted memory sticks are permitted.
Mobile Phones with internet connectivity and/or audio/video/ camera recording functionalities	Not allowed	Not allowed	Patients may be allowed to have their own mobile phones whilst on leave (including unescorted perimeter leave), but must be provided with a Trust mobile phone for use within the ward and this is subject to MDT agreement and some restrictions governing its use.
Dongle, wireless NIC, etc.	Not allowed	Not allowed	These devices allow computers and other devices (including some PDAs, phones and MP3 players) to connect wirelessly to the internet.
Analogue or digital radio	Allowed	Allowed	
Laptop, netbook, PC or other computer	Allowed – ward laptop that does not connect to the internet only	Each ward has a non-networked PC for patient use, which can be used without supervision. Some wards have patient PCs with access to the internet and are located in the communal area	Patients are not allowed to attach any form of external storage device other than a Trust approved and encrypted USB stick that has been issued to patients following MDT agreement (i.e. personal memory sticks, writable CD or floppy disk). Patients can plug in an

			approved MP3 (using detachable USB) in order to charge the battery or copy songs from a music CD. Personal laptops and tablets are not permitted on theward as these devices could connect to the internet using mobile signal through a SIM card.
Camera or video-camera	Not allowed	Under staff supervision as long as a contraband authorisation form has been completed.	Cameras must not be used to take pictures or moving images of patients without signed consent.
CD Player	Allowed	Allowed	Blank CDs are not allowed in patients' bedrooms.
Audio Cassette Player / Recorder	Allowed, provided that there is no attached or integrated microphone to allow recording on the ward	Allowed	
Video Cassette Player / Recorder	Allowed, provided that there is no attached or integrated camera or microphone to allow recording on the ward	Allowed	Video cassettes are not allowed in patients' bedrooms.
Analogue TV	Allowed.	Allowed.	
Freeview or Digital Terrestrial TV	Allowed.	Allowed.	Patients can potentially access pay per view pornographic channels via Freeview. If staff have concerns, parental controls can be used to block offending channels with patient's consent. If consent is not given it may be necessary to remove the TV.
Cable or Satellite TV	Not allowed	Not allowed	
Games Consoles	Consoles that have Wi-Fi connectivity (e.g. infrared, wireless etc.) and/or storage capabilities (e.g. USB memory) are not permitted. Most new consoles (X-Box 360, PS3, Wii, DSi) have these capabilities. Some devices (e.g. DSi) can also take photographs and record voices so would be not permitted on that basis alone.	Consoles with Wi-Fi connectivity or storage capability are allowed on the ward under staff supervision and must be locked away when not in use.	If you are unsure whether a particular console has wire-free connectivity or storage capability, or whether a cable should be detached and kept by staff, have it checked by a knowledgeable member

	Only consoles with no connectivity, storage, photographic or recording capability are		

	allowed, provided unnecessary cables are detached and kept by staff		
DVD Player	Allowed Most new TVs have integrated DVD players	Allowed	Only genuine versions of certificated films and TV programmes allowed on the ward / in patient's bedrooms. Some content may be restricted by clinical teams on a case by case basis. Certificate 18 films cannot be shown in communal areas. Blank or 'pirate' DVDs are not allowed on the ward

10.2 Decision flow chart for determining level of access of technological devices



11.0 COPYRIGHT

11.1 All formats of music and video including cassette, CD, DVD and digital cannot be copied or shared by staff for patients in order to comply with copyright laws (Copyright, Designs and Patents Act 1988). Pirated music and DVDs are illegal and therefore should be dealt with in the same way as contraband items.

12.0 ACKNOWLEDGEMENT

12.1 With permission of the authors, section 9.0 of this policy has been developed (with minor adaptions) from the South West London and St Georges Mental Health NHS Trust's policy – *Managing Patient Access to Technology in the Forensic Service.*

END