Forensic Directorate
John Howard Centre

Inpatient Access to Computers

Version 9.3

East London NHS Foundation Trust

TITLE	Inpatient Access to Computers
PURPOSE OF DOCUMENT	To enable Patients to access computers within the John Howard Centre in order to develop recreational, vocational and educational skills in a safe and secure way.
EXECUTIVE SUMMARY	The policy provides guidance for staff in the management of patients while accessing computers and related hardware. This protocol was initially written in line with the recommendations relating to Computers and IT Security in the Ashworth Inquiry (Appendix 1).
ELECTRONIC FILE REFERENCE (AUTHOR)	I:\JHCPOLICIES-PROCEDURES-PROTOCOLS\POLICIES\Inpatient access to computers.doc Accessible from Policy Index Document at I:\JohnHoward\8. Policies & Procedures
ELECTRONIC FILE REFERENCE (NETWORK OR INTRANET)	I:\JHCPOLICIES-PROCEDURES-PROTOCOLS\POLICIES\Inpatient access to computers.doc Accessible from Policy Index Document at I:\JohnHoward\8. Policies & Procedures
STATUS	Final
VERSION NO.	9.3
DATE OF THIS DRAFT	23.02.18
AUTHOR(S)	Amy Davies
REVIEWED BY	Alison O’Reilly Aug 2021
CIRCULATED TO	SCM
APPROVED BY (NAMES, TITLES AND DATE)	Wolfson House Policy Group 31.03.11
NEXT REVIEW DATE	September 2024

VERSION CONTROL SUMMARY

Version	Date	Status	Comments/Changes
1.0	24/07/09	Final	Agreed by SMDT
2.0	10.08.09	Final	Agreed by SMDT
3.0	10.08.10	Final	Annual review
4.0	21.03.11 05.03.12 June 2013	Final Final Final	Reviewed to include Wolfson House Annual review Annual review
5.0	18.09.13	Final	Inclusion of Millfields stand alone protocol. Introduction of all USB sticks regardless of size becoming restricted items. Size limit increased up to 8GB
6.0	February 2015	Final	Inclusion of ward based tablet computers. Reviewed by: John Wilson, Adrian Salmond
7.0	10.09.15	Final	Final review following review by the Technology and Safety Group.
8.0	05.01.17	Final	Removal of Wolfson House Inclusion of Design & Print computers (Whitbread) Inclusion of Internet Access Group Additional info re. MP3 player restrictions
9.0	03.01.18	Final	Updates re. ward based tablet computers Inclusion of Skype Protocol and forms

			Inclusion of Internet Access Protocol and forms Inclusion of support/maintenance info re. Oasis Social Area PC Inclusion of Patient Laptops including FAQs.
9.1	26.07.18	Final	4.2 Clarification on tablet devices. No longer held by OTs but to be held on wards with Ward Manager as responsible staff member. 5.1.2 Supervised internet access on tablets is permissible 5.3 Section on patient personal laptop computers to complement Appendices 8 and 9 Minor formatting of sections 4 and 5 Appendices 8 and 9: trial removed as this has now ended and policy is fully operational
9.2	24.10.18	Draft	5.1.2: 1-1 supervision required for tablets Appendix 7: Updated laptop induction for staff
9.2	21.12.18	FINAL	5.1.2 General leisure use details
9.3	24.03.20	Draft	1. Clarification re. wireless access 3. Maintenance by Trust IT and clarifications about security issues 4. Clarification about storage and access 5.1.3 Links to current UK copyright 6.3 Clarification re. MP3s and copyright with link 8 Clarification re. internet access Appendices Minor clarifications
	20.04.20	Draft	Replacement of Samsung Tablets with iPads 5.1.2.2 to 5.1.2.6 Updates on tablets (iPads) relating to login, network, setup and service reporting
	13.05.20	Draft	Inclusion of Zoom – similar protocol to Skype but with focus on online meetings such as User Involvement Group. Zoom accounts have been set up for all wards References to use of Zoom for UIG, Recovery College, therapeutic activities
9.4	06.08.21	Draft	Updated Laptop Appendix

1. Introduction

Patients access computers within the John Howard Centre to develop recreational, vocational and educational skills. Computers may also be used to undertake work relating directly to their therapy programme, such as diary work and homework for various groups.

This protocol is written in line with the recommendations relating to Computers and IT Security in the Ashworth Inquiry (**Appendix 1**). The primary risks in terms of computer use would be accessing the internet to download pornography, violent imagery, handbooks that may assist the making of weapons or explosives.

There is also the potential for bullying if patients were to access each other's private writings. In the Ashworth Report it highlighted that patients were potentially accessing technology that was not permitted and were using the ward computers to run businesses from the ward without the full awareness of staff.

There is also the potential for patients to copy and distribute CDs and DVDs which may infringe copyright laws and/or may contain pornographic images. Visitors may be able to smuggle in memory sticks with illicit material on them.

This protocol refers to the use of computers by patients within the John Howard Centre, including in Therapy and Education areas and in designated ward communal areas, and the use of the Internet when on community leave.

No patients are permitted to have computers in their bedrooms, unless it is a laptop permitted by MDT and Security, and the use of patients' own computer hardware is not authorised, unless it is a laptop permitted by MDT and Security.

There is to be no patient access to the internet within the site that is unsupervised by staff.

There is to be no unsupervised patient access to wireless technology or mobile phones within the site, unless it is a) a wireless (but not Bluetooth) peripheral device attached to a Hifi or MDT-approved laptop, or b) a mobile phone permitted by MDT and Security.

The purpose of patients having access to computers is to develop recreational, vocational and educational skills.

This protocol should be read in conjunction with Trust Policies and Forensic Protocols and Procedures.

2. Aims

The aim of this protocol is to:

i) Ensure that patients access computers within the John Howard Centre in a safe and secure manner.
ii) Assist in the management of computer equipment for use by patients.
iii) Provide instruction and guidance for staff on the use of computers by patients.
iv) Allow patients to access internet-based functions in a controlled and supervised manner for the purposes of meeting identified therapeutic, educational or vocational needs

3. Security and Maintenance of Computers and Tablets

Maintenance of patient-accessible PCs in the following locations: Whitbread Education Room, John Howard Education Room, Millfields Library is by Trust IT. Maintenance calls for these PCs can be raised by any staff member via the IT Service Desk Portal, quoting the MH number for the affected PC(s).

Maintenance of patients' personal laptops is provided by a computer company recommended by the Trust IT department (Bridon IT Support Ltd – www.bridon.net). Bridon IT will complete repairs and routine checks on the laptops as and when required. Bridon IT also carry out the "lock down" process on the laptops to make them ready for patient personal use.

No software packages or external devices can be installed on the computers without the use of an administrator's password. The passwords are held by Trust IT or Bridon IT and are not shared with staff members. The password should not be typed in view of any patients. Without the password it should be impossible, for instance, to install devices that would allow for wireless network access.

Regular checks will be completed on the computers. These can examine the programmes used and flag up any misuse. These will be carried out alongside staff from Trust IT or Bridon IT as appropriate.

Staff who facilitate access to a computer should organise seating and equipment so that the screen may be visible at all times. Should a patient be unwilling to comply with this direction, the session is to be terminated and the patient returned to the ward. The staff member should ensure a corresponding clinical entry is made on RIO. It is acknowledged that even with the screen visible, it will not be possible to observe and register every screen/tab accessed, and it is acknowledged that a balance will need to be struck between observation and intrusiveness on the part of the escorting staff.

In the event of observed or suspected misuse of any of the computers, access to the computers will be suspended for an appropriate period and the issue should be reported to the Security Department. If deemed appropriate, a Datix incident report should be completed and the information handed over to the ward staff (if escorting staff are non-ward staff) at the earliest opportunity

It is anticipated that minor violations of the policy may be resolved by 1-1 discussion with the patient and reminder of the policy restrictions. For more serious violations, an investigation into the misuse of the computers should be taken as soon as possible. If appropriate, room searches will be carried out to locate any unauthorised devices, such as unauthorised mobile phones, USB devices or modems. Access to the computers will only be reinstated with the agreement of the MDT.

During routine pat down searches and room searches, staff should be vigilant in looking for restricted or prohibited items relating to information technology.

4. Location/Storage of Computer Equipment

4.1 Therapy Areas

There is computer hardware and accessories, including four desktop PCs (John Warburton Education Room), three laptops (Whitbread Education Room), two desktop PCs (Millfields Library), DVD/CD burners and scanners in the Therapy areas of the site. The use of this equipment is subject to individual group and area protocols. The equipment should be checked and remain in their designated areas at all times unless removed for maintenance or specific purposes. Communication to relevant parties and a record of their location should be made.

There are two iMacs in the Admin Hub in the Whitbread Building. These are only to be used by designated staff involved in the Employment project.

One iMac is installed in the Millfields Library. There is a red lock box, which contains the mouse and keyboard for the iMac. As both are wireless and these are to be kept in East India's nursing station when not in use, and there is a sign out book when they are. The iMac computer is specifically intended to be used by those engaging in Design and Print vocations, for the production of the Millfields Chronicle and Millfields website page.

One iMac is installed in the John Warburton Education Room. The mouse and keyboard for this, which are wireless, are stored in the Education Room filing cabinet.. The iMac computer is specifically intended to be used by those engaging in vocational activities such as music production or design.

One Lenovo ThinkCentre desktop PC is installed in the Oasis Social Area (Whitbread Building). This is connected to the Patient Internet Network, and Trust network login in not possible. Please see **Appendix 14** for instructions and support guidance.

4.2. Tablet Devices

Each ward has an assigned iPad tablet device for use by service users on a supervised basis. The gatekeeper for each device is the Ward Manager for the ward. The devices for the JHC wards are stored in the Nursing Office safe on each ward. The devices can be accessed by staff for use with a service user on a supervised basis, either on ward or off-ward. The device must be signed out of the safe before use and signed in after use.

Any faults on Trust tablet devices should be reported to Trust IT via the IT Service Portal.

4.3 Ward Areas

Wards on site can enable their patients to access a non networked, stand alone PC.

JWB; Elizabeth Fry and Whitbread Buildings

Within these buildings the PCs should be kept in a secure state when not in use and accessed by patients in communal areas such as the ward quiet room or meeting room.

Millfields Unit

There is a non-networked, standalone desktop computer and printer in East India Ward located in quiet room in the communal areas. They should remain in that room at all times unless removed for maintenance or other specific purposes. A record of their location should be made. There is currently open access to this equipment. There is no access to hardware such as scanners or CD/DVD burners.

Access will be reviewed if incidents or issues arise. If there is suspicion that the computers on the ward or the room is being abused the computer room should be locked off. This should be done at ward staff's discretion.

Patients will have access to the printer without direct supervision but subject to random and regular checks of documents printed. Abuse of this facility would result in a review of its provision.

Patients are not allowed to connect any device to the printer other than the designated computer.

4.4 Trust laptops for staff use

Trust laptops that are held on the wards or by departments, and are logged into via staff ID, are not designed to be used by patients, either supervised or unsupervised.

5. Use of Computers by Patients

5.1 Use in Therapy Areas

5.1.1 Access: Groups & Individual Sessions

Individual area and group protocols govern the specific use of computers by patients on site. Access to computers in therapy areas will be supervised at all times. All groups/ departments enabling the use of computers by patients must submit their protocols to the Security Department to ensure safety and consistency in approach.

5.1.2 Use of Tablet Devices

5.1.2.1 The tablet devices can be used in individual sessions with service users for the purposes of meeting an identified therapeutic, educational or vocational need. Access to the device can take place in an on-ward location or in an off-ward therapy area. This is subject to 1-1 supervision at all times. Access to the internet via the Trust network is permissible if required. Devices support the use of applications compatible with the device. These can accessed and used by service users. The authorised categories of usage are as follows:

- Education exercises, tools and information·
- Therapeutic exercises, tools and information
- Vocational exercises, tools and information
- Social activities and places of interest to visit
- Sports and leisure related activities
- Journey planning in relation to community leave
- General leisure use if deemed appropriate – please note that social networking websites that are banned in the Inpatient Access to Computers policy e.g. facebook, may not be accessed. The same applies to associated apps e.g. Facebook Messenger.
- Skype or Zoom calls to agreed family and friends, following guidelines in Section 9 and Appendices 10 to 13
- Participation as service user representative in meetings such as User Involvement Group
- Participation in online Recovery College sessions, either as peer tutor or student
- Participation in therapeutic activities when conducted online

However, this is subject to 1-1 staff supervision at all times.

The devices are not to be used for any unauthorised purposes and abuse of this facility will result in its removal

5.1.2.2 The tablets do not require a personal login from staff or service users (e.g. ELFT network login or Apple ID)

5.1.2.3 the tablets do not have access to any network drives or staff intranet services.

5.1.2.4 Wi-fi and internet connectivity is available to the tablets using the **NHS-WIFI** network. Staff should consult current guidance on use of the NHS-WIFI network.

5.1.2.5 The tablet devices are set up by Trust IT and are pre-loaded with appropriate programs. Restrictions are in place on the tablets to prevent inappropriate use.

5.1.2.6 Any service requests or fault notifications relating to the ward tablets should be raised with Trust IT via the IT Service Desk Portal.

5.1.3 Use of CD/DVD Burning Equipment

Some therapy areas on site have access to CD/DVD burning equipment. Neither patients or staff should use the CD/DVD burner to infringe copyright. This includes the reproducing of music or films that are under copyright. It is not permissible to make back up copies of music or films that are copyrighted under UK copyright law.[1]

[1] https://www.winxdvd.com/resource/dvd-copyright-infringement-laws.htm
https://uk.pcmag.com/copyright/73587/its-illegal-again-to-rip-cds-for-your-own-use

The CDs that are permitted to be burnt are:

1. Backing up computer programmes
2. Storing texts, pictures or photographs
3. Converting MP3 files to audio using appropriate audio software.

All other requests to use the CD/DVD burner should be discussed as part of the specific group and where necessary with the patients MDT.

5.1.4 Use of scanner equipment

Some therapy areas on site have access to scanner equipment. Patients should be supervised at all times when using scanners. Copyrighted images should not be reproduced.

5.1.5 Printing

Patients will not have access to printers without the supervision of staff. Staff must check all materials that have been printed.

5.2.2 Printing

5.3 Patients' Personal Computers

A patient may keep his/her own laptop computer on the ward providing that it is internet disabled, camera disabled and video/audio recording disabled. Prior to bringing the device into the unit, the patient's MDT should consider and approve the request. Before the patient is able to use the device, an external IT contractor (Bridon IT) will check that it is internet disabled, camera disabled and recording disabled and that there are no unauthorised images or recordings stored on, or peripherals attached to, the device.

The patient will need to agree to have restrictions placed on the laptop by an external IT contractor, Bridon IT. These will include: USB access; Bluetooth; wifi; recording (video/audio); burning to DVD/CD.

It may be deemed more suitable by the MDT to permit use in day areas only and for the laptop computer to be treated as a restricted item. In this case, some of the above restrictions (such as USB functionality) may be eased in agreement with the Security department. However, wifi access and recording facilities are likely to be restricted by Bridon IT as a minimum, and the laptop will be kept in a secure location accessible only to staff when not in use.

Please refer to Appendices 8 and 9 for FAQs re. patient personal laptop use.

6. The Use of Memory Sticks, Storage Devices and Saving Materials

6.1 Saving of Patients' Work

If patients' work needs to be saved, the hard drives of the computers must not be used, other than for temporary storage. All work should be saved to a disk or memory stick.

6.2 Use of Unit/ Departmental Memory Sticks for Patient Use

Patients in the following groups will be able to use unit/departmental memory sticks allocated for patient use to save their work. Patients in the following groups may be allocated these memory sticks:

- ICT
- English
- Maths
- ESOL
- Internet Access Group

All of these memory sticks will be allocated individually to a patient and labelled with the patient's initials. When not in use they will be kept securely locked away.

Memory sticks should not be used for any other purposes than the above. Staff are not permitted to remove patient use memory sticks from the John Howard Centre.

6.3 Patients' Personal Memory Sticks/ MP3 players

The use of patient's personal memory sticks/floppy disks will be agreed by the patients MDT. The memory capacity will be up to and including 8 GB.

Any memory stick will be stored in the patient's restricted items box and access will be subject to a signing in/out basis in line with the Prohibited/Restricted Items Protocol.

Anything over 8GB is a banned item and will be kept securely in the patients banned items until disposal thereof.

USB cables are restricted items and should not be given to patients for the purpose of downloading copyrighted content. No MP3 player or other USB device may be used to download copyrighted content unless purchased by the patient from a legitimate source. Accessing websites for converting online content such as YouTube audio to MP3 is strictly forbidden.[2]

Staff are reminded not to download music on Trust PCs for patients.

If suspicions arise, staff should search the contents of any storage device as required.

7 The Use of the Internet on Community Leave

7.1 Escorted Leave

The Internet is now an important part of everyday life. People access the Internet as part of their work, education, leisure and even to carry out activities of daily living such as shopping. In addition, electronic communications through email is now a common form of staying in contact and making

[2] https://www.express.co.uk/life-style/science-technology/970429/Youtube-downloader-convert-youtube-to-mp3-is-it-legal-fined

requests. Therefore it is important that patients, who are interested, are supported to use the Internet as part of their rehabilitation.

Patients who are interested in accessing the Internet and have escorted leave should be supported by staff to teach them how to use the Internet as part of a structured Care Plan discussed and reviewed by their MDT, including discussion about the setting up of free email accounts. There is also potential for patients to set up their own websites and access social networking

Access to the Internet is not without risks as there is a large volume of sites which have pornography, violent imagery, handbooks that may assist in the making of weapons or explosives and other sites that may compromise the safety of the unit. Although most Internet cafes and libraries have parental controls on their machines it cannot be assumed that all will.
When patients are on escorted leave the risks can be managed through the supervision of escorting staff. Feedback about any concerning behaviour should be reported to the patients MDT.

7.2 Unescorted Leave

On unescorted leave the risk issues are greater and consideration to potential misuse of the Internet should be given when applying for or granting unescorted leave.

8. Onsite use of internet

8.1 Access and Uses

8.11 Access to the Internet will be considered carefully, and requests will go through the multi-disciplinary team via CPA Review or minuted Ward Round meeting. Known risks and interests in violent or pornographic material will be highlighted and recorded on a referral and risk assessment form. Patients will be asked to sign a consent form (**Appendix 2**), indicating that they understand the limits of use imposed by this policy if access is granted.

8.1.2 Patients requesting access to the Internet should have valid reasons and these will be considered via CPA Reviews or minuted Ward Round meeting.

These include:

- Those enrolled on study courses.
- Research for activities/interests.
- To visit physical/mental health sites.
- Planning community trips/local information.
- Accessing career/job search sites.
- To stay in contact with relatives if other
- communication is difficult e.g. relatives abroad

Appendix 5 contains a form for a record of patients with current agreed access.

8.1.3 Patients may not have access to the following sites:

- Those deemed inappropriate by the multi-disciplinary team, for example, pornographic sites, sites where telephone numbers or addresses can be sought, professional registers, searches for “names” which may reveal website and contact details, etc. Other prohibited sites would be discussed on an individual basis and made clear to the patient by supervising staff. This information will be recorded on the referral and risk assessment form and stored in a locked cabinet in the John Warburton Education Room or in the safe in the Whitbread Education Room.

- Chat rooms/bulletin boards.
- Facebook, twitter and other social networking sites.
- E-mail sites unless agreed by MDT. If agreed, gmail is the only site that patients are permitted to use. Patients who do not have a gmail account should be assisted in setting one up if required.
- Gambling sites.

Inappropriate sites will be blocked by URL or category. This is done by filtering software installed by Trust IT. Cases of sites that may be accessed but appear inappropriate should be referred to Trust IT via the ICT Service Desk Portal, who can remotely block them.

8.1.4 Patients may not download software of any kind, including upgrades, games, ring tones, etc., to the computer or a disk. Other information may be downloaded with the consent of escorting staff, for example, articles for study purposes. This information is to be printed out and stored on a memory stick and kept in a locked cupboard/safe in the Education room, or kept in the ward safe.

8.1.5 An inducted member of staff who has a good working knowledge of the Internet will closely supervise all Internet sessions. For laptops stored in the Whitbread Education Room, there is a brief induction session for staff to gain access to the safe. This is normally carried out by the Education Lead or ICT Tutor. The induction form can be found in **Appendix 7.** Access will be given during structured session times by approved staff. **Appendix 6** (Session Aims) may be filled out in advance of the session to aid planning and reinforce boundaries. This is at the discretion of the supervising staff. For PCs in the John Howard Education Room, there is an induction facilitated by OT Staff.

8.1.6 Sessions must be booked and the purpose of each session will be planned in advance and discussed with the supervising member of staff.

8.1.7 Use of the Internet will be fairly allocated amongst those with access, but priority will be given to those engaged in courses or undertaking work-focused research.

8.1.8 Misuse of Internet access will lead to immediate termination of the session and suspension of privileges pending discussion at the next Ward Round or CPA Review.

8.1.9 Anti-virus and Internet control software will be installed on each computer by Trust IT. However, if the supervising member of staff becomes concerned at any time about any aspect of Internet use during a session, they must take appropriate action, including stopping the session if required.

8.1.10 Any effort on the part of a service user to access inappropriate material must be reported to the relevant head of department and to the ward staff/MDT as soon as possible. An entry must be made in the Rio progress notes and a Datix incident form completed.

8.1.11 Examples of inappropriate material include pornography, chat rooms (children's chat rooms in particular), social networking sites (i.e. Facebook, Myspace etc.), material and sites relating to racial and religious hatred along with sites on weapons and the making of them (e.g. building explosives), gambling sites or personal e-mails to/from family or victims that have not been authorised by the clinical team. This is not an exhaustive list. Any material that causes the supervising member of staff concern should be responded to in the above manner.

8.1.13 Patients who do not have community leave will be given priority to onsite Internet sessions.

8.2 Staff Responsibilities and Equipment Use

8.2.1 Staff must not use the patient computer to access the Internet for their own personal use. This will enable an accurate “history log” of patient use to be kept. Web histories can only be deleted by Trust IT.

8.2.2 The patient must receive a copy of the Computer and Internet Access Policy Summary (**Appendix 3**) and sign the consent form (**Appendix 2**). Completed **Appendix 2** forms should be stored in the Blue ring binder in the Education Room or Millfields Library.

8.2.3 Internet access will only be available on computers designated for patient internet use.

8.2.4 The connection will be provided by a remote external modem that will only operate on the identified computers. The internet connection is the Patient Internet Network, which is separate from the Trust network.

8.2.5 Staff will prepare the room and check connection to the Internet service before each session.

8.2.6 The date, time, name of patient and supervising staff using the internet should be recorded for every session on the Internet Access Motoring form (**Appendix 4**), to be kept in bound copies in the Education Room or Millfields Library.

8.2.7 Google Chrome and Internet Explorer will retain the history of web pages visited. A history check may be carried out, if necessary, at the end of each session by the supervising member of staff, recorded for audit purposes.

8.2.8 Large reams of material must not be printed. Patients must agree with staff which material is essential before printing. Patients wishing to print more than ten pages per session may be asked to contribute towards the cost. Patients should be made aware that printing a single web page may result in a large number of unnecessary sheets being printed, and that a set number of pages (one or two are normally adequate) should be chosen from the Print Dialog.

8.2.9 Virus checkers, e.g. Avast antivirus should be present and updated regularly by IT staff.

9. Use of Skype and Zoom

9.1 Definition

Skype and Zoom are Internet based services that are free to those who create an account. It enables people to talk and see each other through a webcam.

9.2 Procedure

9.2.1 Service users wishing to use this facility will need to complete the application form (**appendix 10**) and submit it to their MDT to be approved. This will include a list of people the service user wishes to contact and their Skype and/or Zoom addresses. A letter (**appendix 12**) will be sent to the persons on this list to seek their permission for the service user to contact them. No contact will be permitted until this permission has been returned. This could be completed verbally by a member of the MDT. This procedure does not apply to participation as service user representative in meetings such as User Involvement Group or participation in therapeutic activities.

9.2.2 Discussion by the MDT must highlight any issues that need to be managed or given specific consideration during the call and guidance provided to supervising staff. This information must be recorded in the service users care plan and the Risk assessment (**Appendix 11**) should be completed.

9.3 Involving children in Skype or Zoom Calls

If a Service User requests children in their Skype or Zoom Call the request must go to the Children's Visitor Panel as per visiting procedure for children within the service.
It must be highlighted to persons involved in Skype or Zoom calls that only persons approved should be present at time of call and that this includes any children.

9.4 Location of devices for Skype and Zoom

Ward tablets will be used to facilitate the Skype and Zoom calls. Skype and Zoom can be installed upon request to Trust IT, if not already pre-installed. Use of tablets with service users will be continuous supervision at all times in a private room that has been booked. The tablet must be placed within the room in a position that does not allow the camera to view other members of staff or service users, or other features that may be confidential or any security features, including doors or locks.

9.5 Skype and Zoom accounts

Ward accounts will need to be set up for all Skype Calls. Account to be set up as per **Appendix 13** instructions. Patient contact's from approved list can be added to this account. Log-in details to be held and accessed by ward staff and not given to service users.

Zoom accounts have been set up for all wards and should be active and working for regular meetings such as User Involvement Group (when held online).

9.6 Booking a call

9.6.1 With the exception of participation as service user representative in meetings such as User Involvement Group or participation in some therapeutic activities, including cross-ward activities[3], .arrangements to use Skype or Zoom will be similar to service users requesting a visit. A date, time, and name of person or persons to be contacted must be submitted to a qualified member of the ward-based staff at least 24 hours in advance. If an Interpreter is required five working days advance notice is required. Times to be arranged at the discretion of the Shift Co-ordinator.

9.6.2 Calls must be no longer than 60 minutes in length.

9.6.3 The recipient of the call must be contacted to book the time.

9.6.4 A discrete space should be used for the call and provision made for a supervising member of staff to be present throughout.

9.7 Supervision of a session

9.7.1 A member of staff must be available to supervise the call. They must be able to hear the conversation and see the screen. Following the call the member of staff must make an entry in RIO progress notes.

[3] The Therapeutic Cross-Ward Group Provision protocol should be referred to. This notes a range of complications and disadvantages inherent in relying on such technologies, which makes groups based on videoconferencing a less preferable option, or incompatible with some groups. This can be located at I:\JohnHoward\3. Departments\Therapies\SHARED Therapies\Therapies Cross Ward Group Protocol Covid 19.docx

9.7.2 The service user will only be allowed to talk to the person or persons that have been previously agreed by the MDT. People who the MDT have agreed are appropriate for the service user to contact are to be listed on the Approved Visitors list.

9.7.3 As per visiting policy an Interpreter can be booked if deemed necessary by the MDT.
The service will exercise its right to terminate the call immediately if there are any infringements of the protocol or any identified risks.

9.7.4 Any infringements may result in the service user having access to Skype and Zoom withdrawn until further notice. It may be necessary to end the call if staff deem it necessary.

9.8 Examples of reasons to end call

- Service user or friend/family getting angry.
- Inappropriate language.
- Service user talking to someone who is not on the approved contact list.
- Inappropriate images on the screen

List of Appendices

Appendix 1 Recommendations from the Ashworth Inquiry

Computers and IT security

Recommendation 33

3.39.18 We recommend that patients should only be allowed adapted computers connected to a patients' server in their rooms.

Recommendation 34

3.39.19 We recommend:

(a) no modems whether external or internal should be permitted in ward areas;
(b) patients' access to telephones should be limited to:

(i) telephone numbers on the list of the patient's list of approved numbers;
(ii) all telephone calls by patients should be careful monitored, except privileged calls, such as those to legal advisers, in this cases the number should be dialled by a member of staff who, having done so, should retire our of ear-shot, but maintain observation to ensure no other number is dialled;
(iii) telephone points in ward visitors' rooms should be removed;
(iv) permitting external telephone engineers to control the Hospital's telephone exchange should be reconsidered.

Recommendation 35

3.39.22 We recommend that patients are not allowed to have in the Hospital: mobile telephones; personal organizers; palm top computers; hand-helds; laptop computers; and pagers.

Recommendation 36

3.39.28 We recommend that before patients are allowed to have personal computer printers, it is demonstrated that the parallel port to which such a printer must be connected could not also be used for unacceptable devices.

Appendix 2 – <u>Internet Access Patient Consent Form (Formerly: “Form C”)</u>

<u>PATIENT CONSENT FORM</u>

Name:..Ward: ....

Date of Birth:..RIO Number:..

Consultant:..Primary Nurse:..

1. I have received and read a copy of the East London NHS Foundation Trust Forensic Services Patients’ Internet Access and Use Policy Agreement (**Appendix 5**).

2. I understand the terms and conditions of use laid out within this policy and agree to abide by them.

3. I understand that any misuse of the internet will lead to suspension of my access until my next Ward Round or CPA Review where it will be discussed.

Patient Signature:..
.

Date:...

Signature witnessed by staff member:

Sign: ....

Print Name:...

Grade/Discipline:..

Date internet access agreed by MDT (if different):...

Gmail access agreed by MDT? YES / NO

Please place in blue internet folder in the room where internet is to be accessed.

(Page 1 of 1)

Appendix 3 **Summary of Policy Items relating to patient internet use** – all patients signing Appendix 2 must agree to this. An A3 copy should be posted on the wall in the Education Rooms (JWB/Whitbread) and Millfields Library (adapted from former Form B)

East London NHS Foundation Trust
Forensic Services
John Howard Centre

THIS IS A SUMMARY OF THE PATIENT INTERNET ACCESS AND USE POLICY – AGREEMENT

Access to the Internet must be agreed by the multi-disciplinary team via CPA review or Ward Round. Patients must sign the consent form "Appendix 2" indicating that they understand the limits of use imposed by this Agreement.

There is to be no unsupervised patient access to the internet within the site.

There is to be no unsupervised patient access to wireless technology within the site, **unless it is a) a wireless (but not Bluetooth) peripheral device attached to a Hifi or MDT-approved laptop, or b) a mobile phone permitted by MDT and Security.**

Security & Maintenance

- No software packages or external devices can be installed on the computers without the use of an administrator's password. Software should not be downloaded by patients.
- Staff who facilitate access to a computer are to observe the screen at all times.
- In the event of misuse or suspected misuse of any of the computers, access to the computer will be suspended and the issue should be reported to the Security Department.

Use of computers by patients

The main categories of usage are as follows:

- Education exercises, tools and information
- Therapeutic exercises, tools and information
- Vocational exercises, tools and information
- Social activities and places of interest to visit
- Sports and leisure related activities
- Journey planning in relation to community leave
- General browsing of topics of interest
- Use of gmail (if agreed by MDT) to contact friends and family, and to register for educational activities such as distance learning

Patients may not access the following sites:

- Those deemed inappropriate by the multi-disciplinary team for example, pornographic sites, sites where telephone numbers or addresses can be sought, professional registers, searches for “names” which may reveal website and contact details, etc. Other prohibited sites would be discussed on an individual basis and made clear to the patient and supervising staff.

- Chat rooms/bulletin boards
- Facebook, twitter and other social networking sites.
- Email sites unless permitted by MDT.
- Gambling sites.

A log must be kept of the patient’s usage – date, computer used, supervising staff (sheet to be filled in). This is in a bound A4 booklet next to each PC (JWB) or in the safe (Whitbread).

Neither patients nor staff should use the CD/DVD burner to infringe copyright. This includes the reproducing of music or films that are under copyright. It is not permissible to make back-up copies of music or films that are copyrighted under UK copyright law.

Patients will not have access to printers without the supervision of staff. Staff must check all materials that have been printed. Patients wishing to print more than ten pages per session may be asked to contribute towards the cost at a rate of 10p per sheet.

If patients’ work, including video and audio files, needs to be saved, the hard drives of the computers must not be used. All work should be saved to a disk or memory stick.

Use of the Internet will be fairly allocated amongst those with access, but priority will be given to those who do not have community leave and are engaged in courses or undertaking work-focused research.

Patients’ personal memory sticks & MP3 players

- The use of patient’s personal memory sticks/floppy disks will be agreed by the patient’s MDT. The memory capacity will not exceed 8 GB.
- Any memory stick will be stored in the patient’s restricted items box and access will be subject to a signing in/out basis in line with the Prohibited/Restricted Items Protocol.
- Patient MP3 players should not be used to make unauthorised copies of music or video material that is protected under UK Copyright Law.
- Accessing websites for converting online content such as YouTube audio to MP3 is strictly forbidden.

(March 2020)

Appendix 4 Internet Access Monitoring Form – to be completed by escorting staff every internet session

John Howard Centre
Internet Access Monitoring Form
To be completed in accordance with the Internet Access Policy

Patient’s Name	Ward	Supervising Staff	Date	Time On	Time Off	Computer Number	Has patient signed Consent Form?	
							Yes	No

THIS FORM ONLY TO BE COMPLETED BY INDUCTED STAFF

Appendix 5 – Optional form to record internet permissions for each ward

Ward Internet Access List

To be completed in accordance with the Internet Access Policy

Ward Name: ____

Patient's Name	Date internet access agreed (Form A)	Gmail Access?		Date gmail access agreed (Appendix 2)
		Yes	No	

THIS FORM ONLY TO BE COMPLETED BY INDUCTED STAFF

Appendix 6 – Optional Session Planning Form (formerly: Form G)

John Howard Centre

Session Aims for Patient Internet Access

Please keep a record of what you have agreed to do for each session and put it into the Patient Internet Project file.

Name . . . .   Date . . . .

Patient’s aims for this session are:

•

•

•

•

Staff Signature: . . . .

Notes on session:

•

•

•

•

Appendix 7 Induction checklist for Education Room laptops (Oasis) – to be completed during induction to access safe and laptops

Name: ____ **Date** ____________________________

	Signature
I have access to the “Inpatient Access to Computers Policy”, which is located in the Security Index Document on the I Drive (I:\JohnHoward\8. Policies & Procedures)	
I am aware of the requirements for using memory and storage devices as stated in the above policy	
I am aware of the requirements for maintaining confidentiality of patients’ work on the laptops as stated in the above policies	
I am aware of the procedures for laptop maintenance via the Trust IT Portal.	
I have the code for the Oasis Education Room safe and I am aware that this should not be disclosed to others	
I am familiar with the paperwork relating to internet use in the Whitbread (Oasis) Education Room: 1) Pre-and post-session room checks (on top of safe) 2) laptop sign-out and sign in (inside safe door; 3) Internet Session log (inside safe on top shelf).	
I am familiar with the room check procedure for the Oasis Education Room, which is in line with other therapy spaces.	
I am familiar with the procedures for booking the Oasis Education Room and for informing appropriate staff when taking laptops from Oasis Education Room.	

Name and Signature of staff supervising induction: ____

Appendix 8

East London NHS
NHS Foundation Trust

Laptops for Service Users

Service users are able to request to access a personal laptop for use within the ward environment, which may include in their bedroom. The following outlines the requirements for use and how to make this request:

1. Laptops will have separate log-ins installed to enable certain capabilities only - a 'user' login for service user, and an 'admin' login for designated staff.

2. Under the 'User' login the following capabilities will not be accessible:
   - Networks including Internet
   - Inbuilt recording devices
   - Bluetooth

3. The following will be accessible on an individual basis as agreed by the MDT:
   - USB port – for consideration for activities such as Education-based activities

4. The logins and restrictions will be set up by an external IT provider and can be requested via the ward Occupational Therapist, or Head of Occupational Therapy. There is a small payment for this work which the ward will be responsible for. The laptop will be taken off site for a short period – up to one week, for the works to be carried out.

5. Laptops will be subject to random checks to ensure there is no breach of security. Where individuals decline to comply with this process laptops may be removed to banned items (cashiers or safely stored).

6. Laptops may require connection to the internet to obtain updates although regular updates shouldn’t be required. Requests for this can be directed to the ward Occupational Therapist.

7. At present this service is not available for Apple Macs.

8. Prior to discharge a request can be made to unblock the laptop and reconfigure to standard use. This can be requested via the ward Occupational Therapist.

9. The below agreement must be signed to complete the request.

Name:	**Ward:**
The team agree to the above conditions of use for the laptop to be restricted for use. Please confirm if any of the optional capabilities are permitted:	
USB Port	Yes / No
Care plan in place outlining conditions of use – this may include times and location on the ward	Yes / No
Signed by MDT member:	**Date:**
For service users: I agree to the above conditions of use, including that my laptop can be accessed for random searches and updates as required.	
Signed:	**Date:**

Appendix 9 Skype/Zoom Service User Application Form (formerly: Appendix A)

East London Foundation Trust Forensic Inpatient Services

Service user Access to Skype/Zoom

Service user Application Form

Name:…………………………………………..

Date:……………………………………………

I have received and read a copy of the Protocol for Service user Access to Skype/Zoom.

I understand the terms and conditions of use laid out within the policy and agree to abide by them.

I understand that any abuse of this service would lead to suspension of my access until my next MDT Care Review Meeting where it would be reviewed.

Signed:……………………………………

I wish to make contact with the following:

Name:……………………………… Relationship:………………………

Name:……………………………… Relationship:………………………

Name:……………………………… Relationship:………………………

Name:……………………………… Relationship:………………………

Name:……………………………… Relationship:………………………

This form should be attached to the Skype/Zoom Risk Form and uploaded onto RIO document store

Appendix 10 <u>Service user Access to Skype/Zoom Referral and Risk Assessment (formerly: Appendix B)</u>

<u>East London Foundation Trust Forensic Inpatient Services</u>
<u>Service user Access to Skype/Zoom</u>
<u>Referral and Risk Assessment</u>

Name……………………………………………….   DOB…./…./….

Ward……………………………………………….

This form should be completed by the multi-disciplinary team.

Date completed ……………………

Purpose of Skype/Zoom* access:

Consent has been sought and approved from person/s to receive the calls?
Yes / No

The service user has family and/ or friends that are on the approved visitors list?

Yes / No

Is an Interpreter required for the call?
Yes / No

Known Risks:
Are there people on the service users request list that should be excluded?
Yes / No

Access to the Skype/Zoom* is / is not granted under the terms of the policy.

It has been agreed that………………………….………can use Skype/Zoom* to contact (Please list names of those persons approved):-

Permission has been refused for ……………………….……… to contact (Please list names of those persons not approved):-

For the following reasons……………………………………………………………..……………

……………………………………………………………………………………………………….

This form should be kept on RIO in the document store.

Signature of MDT Member …………………………………….

Print Name ……………………………………………

*Delete as applicable

East London NHS
NHS Foundation Trust

Appendix 11 Skype/Zoom Visitor Consent Form Letter (formerly: Appendix C)

East London Foundation trust Forensic Inpatient Services
Service user Access to Skype/Zoom
Skype/Zoom Visitor Consent Form

Dear

_______________________________ has requested permission to contact you using Skype/Zoom*. Please complete and return the consent slip below as soon as possible and note the following points taken from the Protocol for Service user Access to Skype/Zoom*.

- All calls will be supervised by a member of staff.
- Calls may be terminated by staff at any point.
  Examples of reasons to end call:-
  Service user or friend/family getting angry.
  Inappropriate language.
  Service user talking to someone who is not on the approved contact list, including children.
  Inappropriate images on the screen.
- Calls will need to be booked at least 24 hours in advance with ward staff.

Thank you for your co-operation.

…………………………………………………………………………………………

I do / do not wish to receive Skype/Zoom* calls from (name of service user)

If you consent to receive calls and wish to communicate through this method please provide your Skype/Zoom* contact details: __________________________

Please state if an Interpreter is required and you are willing to consent to this:
Yes / No / Not required

Name:______________________________

Signed:_____________________________ Date:_____________

Or Signed on behalf of staff member following verbal agreement of the above:

Signed: _____________________________ Date: _______

Comment

***Delete as applicable**

Appendix 12 Instructions for Skype Account Creation (formerly: Appendix D)

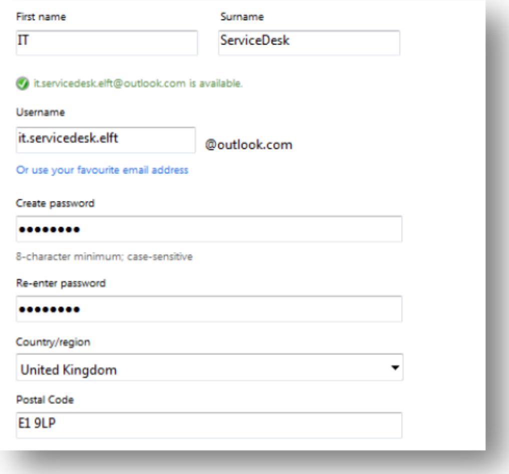
east • london • service • desk

Creating a Microsoft account for use with **Skype**

First, go to: **https://signup.live.com**

Enter your details in the relevant fields

Important, to separate any personal Microsoft accounts (Hotmail.com, Outlook.com, etc) from the one used for Trust business enter your preferred **Username** with the suffix "**.ELFT**" – e.g. it.servicedesk.**ELFT** as below:



First name: IT

Surname: ServiceDesk

✓ it.servicedesk.elft@outlook.com is available.

Username: it.servicedesk.elft @outlook.com

Or use your favourite email address

Create password: ••••••••

8-character minimum; case-sensitive

Re-enter password: ••••••••

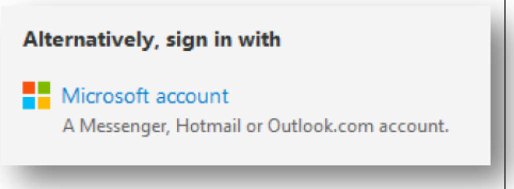
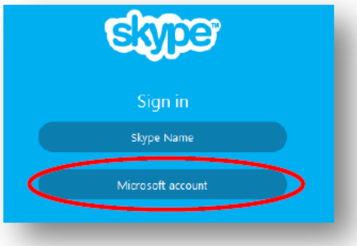
Country/region: United Kingdom

Postal Code: E1 9LP

Also ensure you set-up your personal information such as date of birth and your contact numbers with valid information as you may need this in the future to unlock a forgotten password.

Now enter the validation code and click "**Create Account**".

You can now use this account to sign into Skype choose the Alternative sign in with a "Microsoft Account" either on the Skype Website or application:

Skype Website	Skype Application
 Alternatively, sign in with Microsoft account A Messenger, Hotmail or Outlook.com account.	 skype Sign in Skype Name Microsoft account

This account can also be used on your Trust Windows phone for Store purchases and updates

Appendix 13 INVENTORY FOR COMPUTER & MEDIA CUPBOARD, OASIS SOCIAL AREA

1. Microsoft Wireless 2000 Keyboard
2. Microsoft Wireless 2000 Mouse
3. Wireless receiver (either in mouse or in keyboard – NEVER leave in computer!)
4. 1 x yellow network point plugs (in clear “Lindy” bag)
5. Remote control – Sky
6. Remote control – Sony
7. Remote control – Benq
8. 1 x Network Cable – in jute bag
9. 1 x VGA cable – in jute bag
10. 1 x Audio lead – in jute bag
11. 1 x Lenovo Power lead – in jute bag
12. 1 X LiteOn DVD reader external drive (with connector lead underneath)

IF YOU DON’T HAVE A YELLOW DOT KEY ON YOUR USUAL KEYREEL, YOU’LL HAVE TO TAKE AN APPROPRIATE KEY FROM THE TRAKA ROOM. PLEASE SPEAK TO RECEPTION TO ARRANGE THIS AND FOR FURTHER ADVICE. THIS HAS A YELLOW DOT KEY TO GET INTO THE AV ROOM AND A KEY FOR THE AV CUPBOARD

Using Projector?

1. Lower projector using arrow buttons in AV room
2. Switch on projector using Benq remote (wait 10 seconds for it to fire up)
   NEVER TOUCH/MOVE PROJECTOR DIRECTLY – ONLY USE REMOTE TO SWITCH ON/OFF

Using Lenovo PC?

1. Plug power cable into Lenovo
2. Remove Wireless Keyboard and Wireless Mouse from AV cupboard
3. Remove Wireless Receiver from Keyboard or Mouse and insert in USB slot in PC
4. Connect VGA lead from Lenovo PC to wall socket
5. Switch on PC and log in using “user” as user name and “user” password. YOU WILL NOT BE ABLE TO LOG IN TO YOUR TRUST NETWORK ACCOUNT ON THIS PC AS IT IS CONNECTED TO THE PATIENT INTERNET NETWORK, NOT THE TRUST NETWORK.

Using Trust laptop?

1. Connect VGA lead from laptop to wall socket
2. Connect audio cable from laptop to wall socket (upper double socket). [if audio required]

Need audio?

1. Connect audio cable from Lenovo PC or other device to wall socket (upper double socket). [if audio required]
2. Ensure Cambridge Audio Amplifier (in AV cupboard) is switched on and set to “MP3/Aux”

Need to connect to patient internet?

1. Remove network cable from “Lindy” plastic bag and connect from laptop/PC to available Network point

If you have any problems relating to using a Trust Laptop or the Lenovo PC in this room, please contact Trust IT:

- **020 7655 4004**
- **it.servicedesk@elft.nhs.uk**

If there are any technical problems with the AV equipment in this room, e.g. projector, amplifier, Sky box, DVD player, please contact Optimum:

- **01895 671478**
- **servicedesk@weareoptimum.com**

If there are any problems with key access to the room, AV room or AV cupboard, please speak to JHC reception/security staff.