Mersey Care NHS
NHS Foundation Trust

Policy Number	SS07
Policy Name	Procedure for Service User Internet Access (Specialist Learning Disabilities Division only)
Policy Type	Divisional
Accountable Director	Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Caldicott Guardian
Author	Information and Communications Technology (ICT) Project Manager & Information Governance (IG) Lead
Recommending Committee	Calderstones Clinical Workstream
Approving Committee	
Date Originally Approved	June 2016
Next Review Date	June 2017

This document is a valid document, however due to organisation change some references to organisations, organisational structures and roles have now been superseded. The table below provides a list of the terminology used in this document and what it has been replaced with. When reading this document please take account of the terminology changes on this front cover

Terminology used in this Document	New terminology when reading this Document
Calderstones Partnership NHS Foundation Trust	Mersey Care NHS Foundation Trust

Mersey Care NHS

DIVISIONAL POLICY DOCUMENT

Service User Internet Access (Specialist Learning Disabilities Division only)

Policy Number:	**SS07**
Scope of this Document:	**All staff within Specialist Learning Disabilities Division**
Recommending Committee:	**Joint Information Governance & Caldicott Committee**
Approving Committee:	**Joint Information Governance & Caldicott Committee**
Date Ratified:	**6th June 2016**
Next Review Date (by):	**6th June 2017**
Version Number:	**2016 – Version 1**
Lead Executive Director:	**Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Caldicott Guardian**
Lead Author(s):	**IM&T Security Manager**

DIVISIONAL POLICY DOCUMENT

2016 – Version 1

Quality, recovery and wellbeing at the heart of everything we do

Informatics Merseyside

DIVISIONAL POLICY DOCUMENT

Service User Internet Access (Specialist Learning Disabilities Division only)

Further information about this document:

Document name	**Service User Internet Access (Specialist Learning Disabilities Division only)**
Document summary	**Trust standard on arrangements for service user internet access within the Specialist Learning Disabilities Division**
Author(s) Contact(s) for further information about this document	**Mark Hicks** **ICT Project Manager & IG Lead** **Telephone 01254 821741** **Mark.hicks@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Trust** **V7 Building** **Kings Business Park** **Prescot** **Merseyside** **L34 1PJ** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IM&T Security Standard IT02**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

Version History:		
Draft	**Executive Director of Finance / Deputy Chief Executive / Senior Information Risk Owner (SIRO) / Medical Director / Caldicott Guardian**	**6/6/16**

SUPPORTING STATEMENTS

this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and vulnerable adults, including:

- being alert to the possibility of child/vulnerable adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/vulnerable adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or vulnerable adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

Contents

Index	Page No

1. PURPOSE AND RATIONALE

1.1 **Purpose -** This procedure outlines the processes undertaken to ensure Service Users/Patients receiving care within the Specialist Learning Disabilities Division have access to the internet for the purpose of productivity and leisure activities and as part of rehabilitation. It establishes the responsibilities of staff involves in agreeing and supporting internet access, and the responsibilities of service users when using the IT suites.

1.2 **Rationale** – The Trust aims to provide a least restrictive approach to supporting service users within the Specialist Learning Disabilities Division in accessing the Internet. This support involves assessing the potential risks posed to the service user and others by internet access on an individual basis, agreeing the appropriate level of access with the service user and having clear controls in place to ensure usage remains in line with the jointly agreed parameters. Internet is available to all service users via IT Suites in Gisburn Lodge, Woodview, West Drive, Maplewood and Our Shared College. Internet access in these areas is only available under the supervision of trained staff who will closely monitor the Service User/Patient's activity.

1.3 These services connect to the internet through a data link that is protected by a firewall to prevent unauthorised inbound connection from the internet. The firewall also applies a basic level of internet filtering that prevents access to illegal or extreme/high risk content. This filtering is configured by ICT with guidance from Forensic and High Support Service management on the categories that are blocked.

The IT Suites can be configured for additional website blocking as required using Netsupport software.

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

2.1 For this security standard the aims and objectives are as follows:

(a) To act as a reference for staff and service users on how the Trust supports use of the internet within the Specialist Learning Disabilities Division
(b) To ensure the use of Internet by service users within the Specialist Learning Disabilities Division is conducted safely and securely
(c) To ensure where appropriate that internet access complies with specific restrictions or risk considerations for example the Sex Offences Prevention Order, MAPPA, cyber stalking, etc.
(d) To ensure clinicians involved in risk assessing and agreeing service user internet access within the Specialist Learning Disabilities Division are informed of the process around Service User Internet Passports
(e) To ensure staff facilitating service user internet access sessions within the Specialist Learning Disabilities Division have sufficient guidance to support service users using the internet
(f) To ensure all staff involved in the process within the Specialist Learning Disabilities Division are aware of sources of support
(g) To ensure compliance with related legislation.

3. SCOPE

3.1 All staff involved in agreeing, supporting or facilitating service user internet access within the Specialist Learning Disabilities Division. Note that the processes described in this document and the associated technical services do not apply beyond the Specialist Learning Disabilities Division. For other divisions please refer to SS05 – Service User Internet Security Standard.

4. DEFINITIONS (Glossary of Terms)

Glossary of Terms	Definition
CareNotes	The care records system used in the Specialist Learning Disabilities Division
Firewall	A network security device that acts as a gateway for connections to and from the internet allowing granular control and restriction of both inbound and outbound connections.
MDT	Multi Disciplinary Team
NetSupport	Name of the software application that is used to monitor and control service user internet access sessions
PC	Personal Computer
Web filtering	The practice of restricting access to inappropriate websites

5. DUTIES

5.1 Multi-Disciplinary Team responsibilities

Prior to service users/patients accessing the Internet the Multi-Disciplinary Team will:

(a) Support service users in requesting access by following the Protocol for Service Users Accessing the Internet Using Trust IT Suites. Detail on this is provided in Appendix A of this document.
(b) Discuss and assess service users/patients risks, involving the service user in the process as appropriate. Further supporting information for risk assessments is provided in Appendix B of this document.
(c) Detail agreed levels of access in a service user Internet Passport. A template is provided in Appendix C of this document.
(d) Review access levels as part of the monthly MDT review process. (See appendices B, C and D for further information). The risk assessment and a copy of the service user's Internet Passport will be documented in Carenotes

5.2 Responsibilities of Occupational Therapy staff and other staff supporting service user internet access sessions

As part of facilitating access sessions, staff will:

(a) Provide first line support to service users/patients in connecting to and using the internet
(b) Use the NetSupport software to supervise and monitor service user activity throughout the session and ensure that it remains in line with agreed access defined in the Service User Internet Passport
(c) Restrict sessions where appropriate and support the service user in explaining the reasons for this
(d) Follow appropriate channels for further technical support as needed
(e) Report any suspected security incidents or breaches or inappropriate activity discovered through the appropriate channels, including providing supporting information for any subsequent related investigation.

Supporting information for staff is provided in Appendix D of this document.

5.3 **Management responsibilities**
Managers will ensure that staff are aware of and understand this procedure, ensuring that they have the appropriate skills and training and are updated in regard to any changes to the Procedure.

5.4 **ICT Department responsibilities**
The ICT Department will provide supporting services relating to the provision and technical support of the NetSupport system, PC hardware and network services that are used in IT suites for service user internet access.

6. PROCESS

6.1 Service Users requesting access the internet must follow the Protocol for Service Users Accessing the Internet Using Trust IT Suites (see Appendix A of this document)

6.2 Multi Disciplinary Teams supporting access requests should conduct a comprehensive risk assessment with the service user's involvement, document agreed access using the Service User Internet Passport and upload this to the Trust CareNotes system as a reference. (See appendices B to D of this document)

6.3 Staff supporting service user access must ensure service user internet access sessions are adequately supported and that any incidents or breaches are effectively managed. (See appendix E of this document).

7. CONSULTATION

7.1 This standard has been produced in collaboration with:

- Responsible Clinicians (RCs)
- Occupational Therapy Managers
- Information Governance
- IT Security and IT Network specialists
- Security Managers

8. TRAINING AND SUPPORT

8.1 **Training:**
Training has been provided to key staff on the use of Netsupport Software in the IT suites. Staff are expected to cascade this training to colleagues as required. **Only staff who have received appropriate training will be able to facilitate sessions.**

Staff requiring additional training should contact ICT to discuss this. If third party supplier-led training is necessary the requesting department will be expected to fund it.

Service users requiring training on using the internet should raise this through their care teams. The Trust's ICT department will liaise with care teams to identify options but are not responsible for training service users

8.2 **Support:**
Session facilitators/staff will provide face to face support as required to service users in accessing and using the internet.

MDT will be responsible for any support decisions regarding appropriate use.

The ICT Service Desk will be responsible for dealing with system faults but should not be expected to provide support to service users in using the internet. Any requests for support from ICT should be made via telephone on 3690 or using the fault logging form on the Sharepoint intranet home page. Faults logged with the ICT Service Desk will be subject to the normal ICT support level agreement process. In-person visits without prior arrangement will not be supported unless in an emergency.

For support in investigations contact the IT Security Manager.

9. ACCEPTABLE USE

9.1 Levels of access

The Trust's least restrictive approach takes the stance that Service Users should benefit from internet access unless this would be create unacceptable risk(s).

If there is no prohibitive risk:

- Service users in medium secure services can access the internet under supervised conditions in the Trust's ICT suites.

It is the responsibility of the MDT to determine the level of risk. When a decision is made to limit internet access this must be justifiable and fully documented as detailed in Appendix B of this procedure. MDT may decide to either limit or fully deny internet access as shown in the table below. The level of access permitted should be documented as part of the risk assessment process.

Service user area	Risks identified	Internet access
Low/enhanced	None	OK
	Significant risks	OK
	High risks	No access
Medium	Significant risks	OK
	High risks	No access

This approach results in three possible scenarios for a service user:

Status	When this applies	Access via
Unrestricted internet access (subject to network level restrictions)	- Default position for low secure/ enhanced services (if there are no identified risks)	Access permitted in IT suites
Restricted internet access	- Default position for medium secure (if there is no high risk) - May apply to low secure/enhanced services if there are identified significant (but not high) risks	Access permitted in IT suites
No internet access	- Applies to any service user regardless of service if high risks are identified	None

9.2 Service User Conduct

It must be made clear to service users/patients prior to accessing the internet that misuse may result in access being revoked subject to review by MDT.

9.3 **Session Facilitator/Staff Discretion**

- The session facilitator or other staff supporting the service user/patient will as necessary need to make decisions on what is or is not permissible use of Internet and this will depend on the individual service user's risk profile as determined by MDT. Some examples of what may be deemed offensive can be found below:-

    - Hostile text or images
    - Any content that discriminates in relation to race, gender, sexual preference, disability, political or religious beliefs or any other discrimination
    - Pornographic content
    - Violent content
    - Content considered extremist or supporting criminal activity
    - Content related to computer hacking
    - Illegally copied or "pirated" content
    - Any other content that may be illegal in nature

  Service users must also be prevented from accessing any content that constitutes a specific risk that may be unique to them as highlighted by the MDT risk assessment.

  (These are published in this procedure for guidance only.)

9.4 **Service users/patients must not:**

- Access the internet if they have been restricted from doing so following an MDT risk assessment.
- Access any services or material that would be considered detrimental to their therapy and care as documented following MDT risk assessment.
- View inappropriate content such as that described in 9.3 above
- Publish or make available Personal/Patient or commercially sensitive data.
- Access the Internet under any username other than user's own.
- View and/or send offensive, defamatory or illegal material or breach confidentiality of individuals or the Trust.
- Misrepresent the Trust
- View offensive or illegal material or material that is abusive or threatening to others, serves to harass or bully others or view websites that are designed to cause distress, inconvenience or anxiety.
- Create or transmit any offensive, obscene or indecent images, message, data or other material
- Use or copy any copyrighted material unless in accordance with copyright law (Copyright Designs and Patents Act 1988)
- Purchase anything from any internet site unless this has been approved by MDT. Any purchases the Service User/Patient wishes to make should be discussed with MDT first.
- Make use of the internet facility for personal commercial activities (unless these have been formally endorsed by MDT)
- Make use of the internet facility for political activities

Additionally when using IT Suite computers to access the internet service users must not download or install software onto a suite computer or otherwise attempt to modify the computer configuration

9.5 **Action taken in the event of breaches of conditions:**

It is possible that offensive web sites may be visited by accident or started automatically. If this happens, the service user must exit the Internet browser immediately and notify the session facilitator/staff who will investigate and take appropriate action.

Intentional unacceptable use or any other intentional breach of the established conditions will result in the service user's access being immediately terminated. The service user must not be permitted to access the internet again unless an MDT decision is made to reinstate access following a further risk review.

The session facilitator/staff discovering the breach of conditions will:

- Report the details of any breaches to line management and peers/colleagues including on handover.
- Add an alert to CareNotes to record that the service user's access has been revoked.
- (Where a service user uses their own equipment to access the internet) confiscate this equipment and inform the service user that they cannot have it back until MDT has given approval.
- Any breach that is deemed to be a security incident must also be reported via the Trust incident reporting procedure.

Line management/MDT will

- Ensure the detail of any breach or incident is presented to the next ward round/MDT review for discussion and risk assessment purposes
- Determine whether any investigation is necessary and liaise as appropriate with the parties that need to be involved.
- If there is any suspicion of illegal activity the appropriate line manager will also notify the Trust's Security Manager who will assess the situation and inform the police and/or other relevant bodies as appropriate.
- If the service user's equipment needs to be inspected by ICT to support an investigation this should be arranged with the IT Security Manager.

If warranted the findings will be subsequently reported to the Board, the NHS Security Incident Reporting Scheme and/or the HSCIC Information Governance Incident Reporting tool.

10. Appendix A: Protocol for Service Users Accessing the Internet Using Trust IT Suite(s)

- All service users/patients will be required to request access and wait for MDT approval before accessing any of the IT equipment for the first time.

- The service user's/patients request for internet access may be revoked if necessary following a formal risk assessment by the MDT. The risk assessment should reflect the wide range of risks that may be posed by internet access and relate this specifically to the individual service user's needs and risk profile. (see appendix B).

- The risk assessment and resulting decision must be formally recorded in the Individual Risk Profile Form in the service user's/patients CareNotes record. As this status may change, alerts should be used to inform care staff of the current status.

- It is the responsibility of the multi-disciplinary team to ensure that relevant care staff are aware of whether the service user/patient is permitted to access the internet; this status should be circulated amongst the care team rather than simply relying on the CareNotes entry. This is necessary to ensure staff are aware in real time when access is granted, revoked or reinstated.

- Any service user/patient suspected of or found to breach the service user agreement will have their access to the IT facilities suspended until this can be discussed within individuals' MDT meetings and a repeated risk assessment can be conducted.

- All service user's/patients will be signed in and out of the IT room and details of the number of the computer they are using will be documented within the security checklist books.

- Service user's/patients will be required to enter their name on session commencement and their activity during the session will be recorded in an audit trail.

- All sessions will be supervised by an adequately trained member of staff. Trained staff are expected to cascade training to colleagues.

- A report of all service user/patient activity can be requested by MDT and will be produced by the ICT department.

- If specialist technical support is needed service users should ask the supporting staff to contact the ICT Service Desk on their behalf rather than contacting the service desk directly.

11. Appendix B: Supplementary Information for Risk Assessment

The service user's individual "risk profile" will be considered by MDT and should be treated as a thorough risk assessment around the service user's internet access, based on a least-restrictive approach and tailored to the individual service user.

It must be understood that the generic blocking that is in place applies to all users and cannot be tailored to meet individual service user risks. Where access is granted it is the responsibility of supervising staff to ensure individual risks are managed.

The risk assessment should be actively included as part of ward round discussions. MDT should use the CareNotes Individual Risk Profile Form to record the discussions and the decision on whether access has been granted. The risk assessment should detail in the narrative any restrictions that apply to the service user's potential internet activity so that it can be used as a reference by staff supporting the service user during internet sessions. Alerts may also be used as appropriate to highlight this decision and the service user's care team. Any mention of internet access in the ICP should reference/link to the recorded risk.

This risk assessment should be seen as an evolving process that is discussed and changed in line with the service user's specific situation and needs.

The person(s) assessing risks will need to consider each service user's unique needs taking into account any relevant factors such as SOPO or MAPPA, cyber stalking, stalking etc.

EXAMPLE THEMES TO CONSIDER

- Risks to the service user from the internet
    - Exposure to internet content that may undermine therapy or cause distress
    - Confidentiality and taking care not to post personal information online
        - Cyber-crime e.g. Fraud; Identity theft; Hacking; Cyber-stalking/cyber-bullying; Viruses

- Risks to the general public or the Trust that may be posed by the service user having access to the internet

EXAMPLE AREAS TO CONSIDER

Communications	Internet/cloud based content
• E-mail • Instant messaging • Internet based telephony • Video conferencing • Peer to peer activities (e.g. file sharing)	• Inappropriate content • Gaming (in game communications, content ratings etc) • Applications & programs • Multimedia streaming services • Onine storage • Discussion forums, blogging and social media

Important: These are examples, not an exhaustive list. Other factors or services should be included as required to tailor the risk assessment to the service user's needs. Technical advice can be sought from ICT if the MDT is unclear about any specific technological risk.

12. Appendix C: List of categories to consider when risk assessing service user access

- Art / culture
- Blogs/personal pages
- Business / economy
- Computers / internet
- Education
- Email
- Entertainment
- Fashion
- Games
- General
- Government / military
- Greeting cards
- Health
- Instant chat
- Instant messaging
- Job search / careers
- Lifestyle
- Lingerie and swimsuit
- Media Sharing
- Media Streams
- Nature / conservation
- News / media
- Newsgroups / forums
- Non-profits
- Nudity
- Political / legal
- Real estate
- Recreation
- Religion
- Search engines / portals
- Sex education
- Shopping
- Social Networking
- Software downloads
- Translation
- Travel
- Vehicles

13. Appendix D: Sample Service User Internet Passport

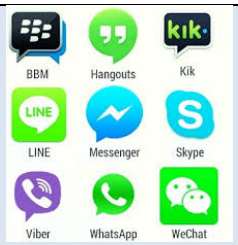
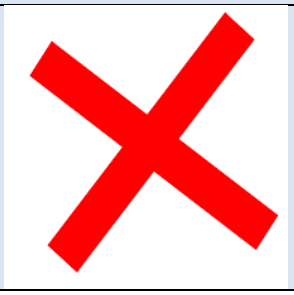
The template for the service user Internet passport can be found at:

G:\(Common Tools)\CareNotes\Templates\Service User Internet Passport.docx

<table>
<tr>
<td>Passport
to the Internet
   </td>
<td>Date agreed by MDT:

My OT is:</td>
</tr>
<tr>
<td colspan="2">I can access the internet under supervision within the ICT Suites</td>
</tr>
<tr>
<td>I understand I cannot access the sites listed in red. My internet access might be stopped if I go on these websites.</td>
<td>

- **Instant messaging**
- **Lingerie and swimsuit**
- **Nudity**
- **Blogs / personal pages**
- **Instant chat**
- **Social Networking**

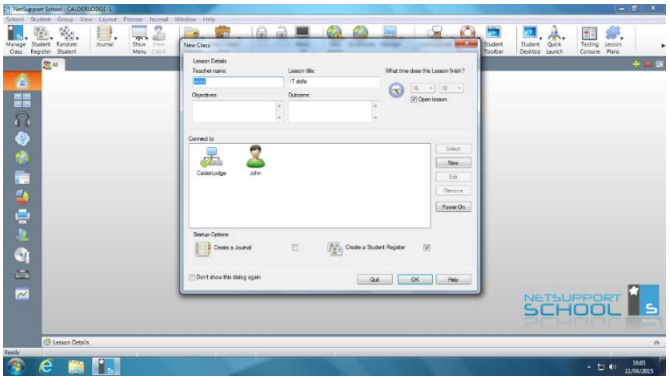
</td>
</tr>
<tr>
<td colspan="2">     </td>
</tr>
</table>

14. Appendix E: Guidance for IT Suites: "Service User Internet Access via NetSupport"

Service User Internet Access via NetSupport

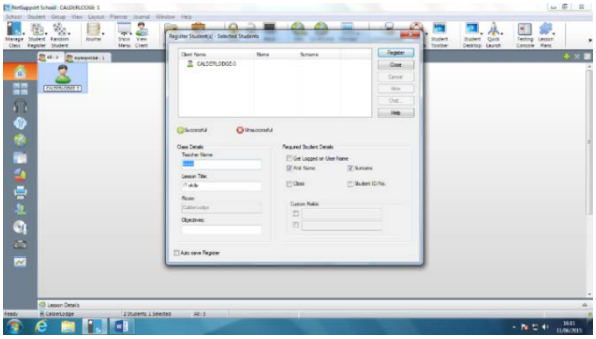
(a) Staff should log onto the Tutor Computer. This should be clearly marked in each area. Choose the log on 'OT'. The password is provided to all staff that need it. If you are not sure, ask a colleague.

(b) NetSupport should automatically launch itself. When this dialogue box comes up choose **OK**. If NetSupport does not automatically lauch, choose the "NetSupport School" Icon to launch it.

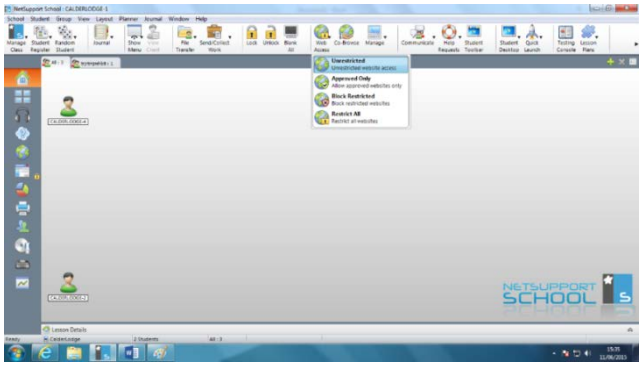


(c) Service users should log onto a PC. One staff can supervise up to three service users provided that supervision levels are maintained at all times and monitoring systems take place. Where there is one staff they should place themselves where they can monitor the service user screens and provide support. Where there are two or more staff, one staff should monitor from the Tutor Computer screen, whilst the other staff should be available to support the service users if they need help. When the service user selects the internet explorer icon they will go straight into a Bing search.

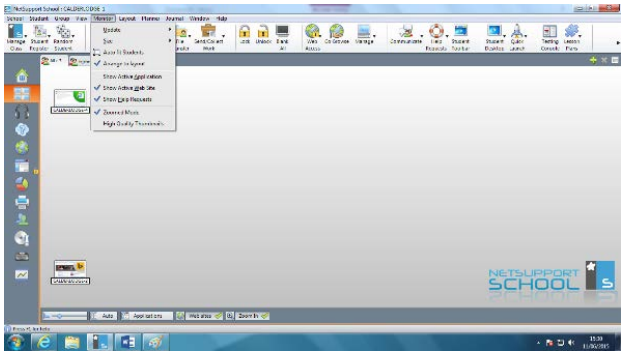
(d) Ask the service user to Register by choosing the **Manage Class** icon on the top tool bar and then select **Register.** This will then present the service user with a Command box on their screen asking them to enter their name. It is important that a separate record is kept of the name of the service user and the PC they have accessed. This can be done in the Service User Equipment Inventory and Supervision book that should be available in each room. Once the service users have Registered you can Close this window.



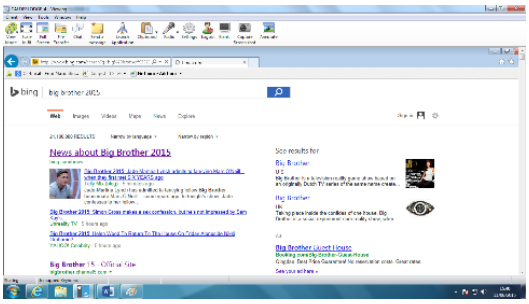
(e) Select level of **Web Access** (see across) – this may vary between groups/individuals and will be informed by the MDT risk assessment. You can do this by selecting the icon or the computer the service user is on.



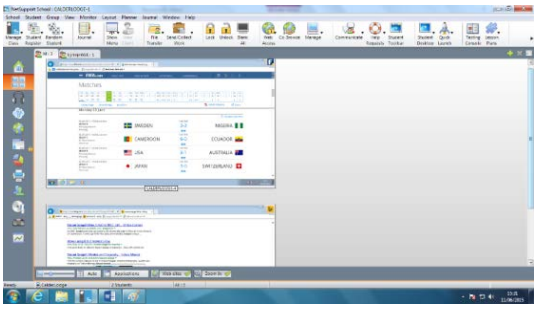
(f) In order that you can monitor the service user screens, select the **Monitor** icon (shown across). If you need to make the screen shots larger choose the **Auto Fit Students**



(g) If you have any concerns about the nature of the search terms or the site that the service user has accessed then double click on the monitor shot of that service user and choose the Blank command from the tool bar.

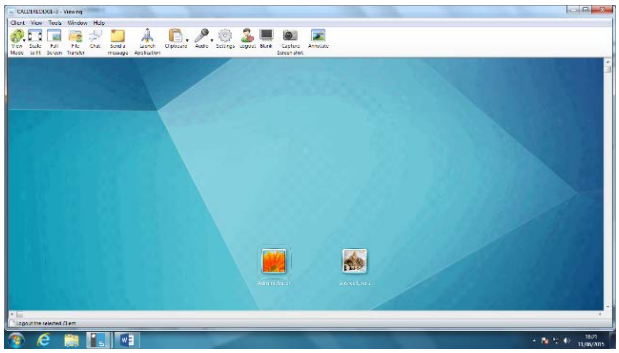


(h) (If you want to manage two or more service user's screens in the same way then choose the Blank All command from the tool bar). To remove the Blank effect click again on the Blank/Blank All icon.



(i) You may also chose to **Log Out** the service users if you have continuing concerns about their activities on NetSupport

(j) At the end of the session ask the service users to log off before you log off from NetSupport. You can do this in the way you would normally log off a Trust PC.



(k) If you observe any risk behaviours (e.g. accessing web sites or entering search terms which are inappropriate) then report this to the shift leader and enter a Cause for Concern on Care Notes.

Trouble shooting:

Access: Sometimes the service user struggles to gain access to the internet. Check that their access is not restricted by selecting their computer from the monitor screen and then selecting the **Web Access** icon from the top tool bar.

Printing: It isn't always possible for service users to print out work. If they have tried without success ask them if it is possible that they wait until their next OT internet session to print out.

15. Appendix F: TECHNICAL INFORMATION

15.1 Web filtering

Web filtering is in use on the network firewall that connects to the internet. The firewall is controlled within ICT and is regularly updated to implement a base level of blocking of websites containing illegal or extreme content. The categories that are blocked will be determined by clinical leads who will liaise with ICT to ensure technical configuration is aligned with clinical guidance.

Users are prevented from accessing blocked sites and any access attempt will instead display a message alerting stating that access is blocked. This blocking cannot be bypassed.

If any changes to blocking are required (for example if a legitimate site is discovered to be blocked) the session facilitator/staff should request unblocking via the ICT helpdesk but should be aware that an immediate response is not guaranteed depending on ICT workload.

15.2 Monitoring activity in IT Suites

Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Trust can lawfully monitor Internet activity for the following purposes:

- Gaining routine access to communications
- Monitoring standards of service and training
- Preventing or investigating misuse
- Unauthorised use of systems (authorised use of Internet is set out under the user responsibilities section of this procedure)
- Establishing the existence of facts
- Ascertaining compliance with regulatory standards
- Ensuring the security of the system and its effective operation

Individual user activity logs can initially be examined by session facilitators/staff on IT Suite computers that accessed the internet. Within the IT suites logs of service user sessions are recorded under the name that the service user used to sign in. Support is available from ICT as required.

Where user activity needs to be investigated consent will be sought if possible but this may not always be the case depending on the circumstances that have led to the investigation. In appropriate circumstances user activity may be investigated without consent, provided there is a justified and legal basis for doing so (e.g. for preventing or investigating crime pursuant to section 29 of the Data Protection Act 1998). The basis for such examination without consent will be documented by the investigating party.

15.3 Anti-virus software

Anti-virus software is installed on IT Suite computers and other Trust owned computers and automatically updates virus patterns daily. If the session facilitator/staff suspects that the PC may be infected by a virus they must contact the ICT service desk for support.

For the purposes of this procedure it is assumed that session facilitators and staff will support the service user in their awareness of general internet safety and associated risks.

15.4 “Netsupport” system

The Trust uses a system known as “Netsupport” to control and monitor access in the IT suites. The system allows multiple PCs to access approved internet resources with control software installed on a different PC that staff can use to enable or block access as required. The control PC offers a way to monitor activity on all suite PCs at once as large thumbnail images on a single screen display. As necessary the staff can zoom in on any session and take control, lock

the session or disconnect if necessary. Other functionality is also available such as the ability to block specific internet sites or programs as well as some functions designed as teaching aids. The computers also use a product "NetProtect" that prevents modifications to each computer's configuration and installed programs.

15.5 **Passwords**

The control PC is protected by a password that should only be known by staff. Computers in Netsupport enabled IT Suites are configured so that they cannot connect to the internet unless the control PC is active. This prevents the controls being bypassed.

Service users use a common username and password to log into the computers. Optionally for larger groups, the Netsupport system supports a "student register" function which, when enabled, includes an additional prompt on start-up for the service user to enter their name. This name will be displayed alongside their activity during the session and helps staff using the control PC to more easily identify which service user is operating each PC.

15.6 **Downloads**

Service users/patients or staff will not be able to install software onto PCs. If any alteration or additional software is required this should be arranged with the ICT support desk.

Other types of files such as documents or PDF files are downloadable as long as they do not contravene the rules around content established in this policy.

15.7 **Website blocking within Netsupport**

Additional filtering can be controlled within the Netsupport software and can be applied by session staff as required to individuals or groups to block unwanted sites based on individual risks.

16. MONITORING

16.1 Records of risk assessments will be updated monthly by MDT and recorded on the CareNotes system

16.2 Audit trails of internet activity will be automatically created during access sessions and stored on the PC being used for access; further activity information is stored on the network firewall logs

16.3 Records of any incidents or breaches will be kept on the Trust's incident management system

17. EQUALITY AND HUMAN RIGHTS ANALYSIS

(analysis template to be completed is included on the next page and must be completed for all policy/procedure documents)

Equality and Human Rights Analysis

Title: **Service User Internet Access (Specialist Learning Disabilities Division only)**
Area covered: **Service user internet access at all IT Suites in the Specialist Learning Disabilities Division (Whalley, Gisburn, Scott House sites)**

What are the intended outcomes of this work? *A framework for effective and safe service users' access to the internet.*
Who will be affected? *Service users, staff and clinicians*

Evidence
What evidence have you considered?
Disability (including learning disability)
Sex
Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.*
Age *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.*
Gender reassignment (including transgender) *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.*
Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.*
Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.*
Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.*
Carers *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.*
Other identified groups *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.*
Cross Cutting *implications to more than 1 protected characteristic*

Human Rights	Is there an impact? How this right could be protected?
Right to life (Article 2)	*Use not engaged if Not applicable*
Right of freedom from inhuman and degrading treatment (Article 3)	*Use supportive of a HRBA if applicable*
Right to liberty (Article 5)	
Right to a fair trial (Article 6)	
Right to private and family life (Article 8)	
Right of freedom of religion or belief (Article 9)	
Right to freedom of expression **Note: this does not include insulting language such as racism (Article 10)**	
Right freedom from discrimination (Article 14)	

Engagement and Involvement *detail any engagement and involvement that was completed inputting this together.*

Summary of Analysis *This highlights specific areas which indicate whether the whole of the document supports the trust to meet general duties of the Equality Act 2010*
Eliminate discrimination, harassment and victimisation
Advance equality of opportunity
Promote good relations between groups

What is the overall impact?

Addressing the impact on equalities

There needs to be greater consideration re health inequalities and the impact of each individual development /change in relation to the protected characteristics and vulnerable groups

Action planning for improvement

Detail in the action plan below the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system, OGDs, other agencies, local service providers and regulatory bodies*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of DH strategic equality objectives.*

For the record

Name of persons who carried out this assessment:

Date assessment completed:

Name of responsible Director:

Date assessment was signed:

Action plan template

This part of the template is to help you develop your action plan. You might want to change the categories in the first column to reflect the actions needed for your policy.

Category	Actions	Target date	Person responsible and their area of responsibility
Monitoring			
Engagement			
Increasing accessibility			