NHS
Birmingham and Solihull
Mental Health
NHS Foundation Trust

ICT Remote Access Policy

Policy number and category	**CG20**	**Corporate Governance**
Version number and date	**5**	**January 2021**
Ratifying committee or executive director	**Trust Clinical Governance Committee**	
Date ratified	**May 2021**	
Next anticipated review	**May 2024**	
Executive director	**Executive Director of Finance**	
Policy lead	**Head of ICT**	
Policy author *(if different from above)*	**ICT Technical Specialist**	
Exec Sign off Signature (electronic)	DB Tomlinson	
Disclosable under Freedom of Information Act 2000	**No**	

POLICY CONTEXT

Birmingham and Solihull Mental Health Foundation NHS Trust (BSMHFT) aims to maintain the confidentiality of all its information including that accessed using the Trusts remote access solution. The conditions set out in this policy aim to ensure this happens.

POLICY REQUIREMENT

The objectives of the ICT Remote Access Policy on remote working:

- Ensure information security and confidentiality when using remote access.
- Understand the risks of using remote access in non-Trust locations and take sufficient steps to reduce or eliminate the risk of data lost through printing, theft of Trust equipment and increase personal security.
- Ensure secure and resilient remote access to the Trust's information systems.
- Maintain the security of organisational information processing facilities and information assets, when accessed by third parties.

Table of Contents

1. Introduction

1.1. **Rationale** (why):

Remote access by staff and other non-NHS organisations is a method of accessing Birmingham and Solihull Mental Health Foundation Trust (BSMHFT) electronic files and ICT systems. This document sets out the policy for remote access and includes a set of common controls, which will be applied to reduce the risks associated with a remote access service.

The object of this policy is to ensure information security and confidentiality when using ICT remote access systems. This policy sets high level controls and is designed:

- To ensure secure and resilient remote access to Trust information systems
- To maintain the security of organisational information processing facilities and information assets, when accessed by third parties.

1.2. **Scope** (Where, When, Who)

This policy covers remote access for BSMHFT staff and other non-NHS organisations to the Trust network, systems or applications i.e. viewing, amending, storing or creating of any information that relates to Trust business on ICT systems.

This policy must be adhered to at all times whenever any user makes use of portable computing devices or uses the remote access portal.

1.3. **Principles** (Beliefs)

- To provide secure and resilient remote access to the Trust's information assets/ systems.
- To preserve the integrity, availability and confidentiality of the Trust's information and information systems.
- To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.
- To comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the Trust is adequately protected under computer misuse legislation.
- Positively support individuals with learning disabilities and ensures that no one is prevented from accessing the full range of Mental Health services available. Staff will work collaboratively with colleagues from learning disabilities services and other organisations, in order to ensure that service users and carers have a positive episode of care whilst in our services. Information is shared appropriately to support this.

2. The Policy

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by BSMHFT:

- Ensuring that all members of staff and all third-party organisations are aware of and comply with the relevant policies
- Describing the principles of security and explaining how they shall be implemented in the Trust.
- Introducing a consistent approach to security, ensuring that all members of staff understand their own responsibilities.
- Creating and maintaining within the Trust, a level of awareness of the need for Information Security as an integral part of the day-to-day business.
- Ensure information security and confidentiality when using remote access systems.
- Understand the risks of using remote access in non-Trust locations and take sufficient steps to reduce or eliminate the risk of data lost through printing, theft of Trust equipment and increase personal security.
- Ensure secure and resilient remote access to the Trust's information systems.
- Maintain the security of organisational information processing facilities and information assets, when accessed by third parties.
- Ensure that all staff and third-party organisations provided with the Trust remote access solution agree to and sign the appropriate Remote Access Acceptance Form.
- To ensure any incidents are reported and actioned appropriately.
- Accessing the Trust ICT network is not permitted from non-trust devices/ systems for staff or third-party organisations without approval from ICT, see **Appendix 4**.

3. The Procedure

3.1. Remote Access for BSMHFT Staff

The Trust currently operates two remote access solutions for staff, Direct Access (DA) and Remote Desktop:

Remote Access via Direct Access

- The Trust manages its remote access through the use of an end-to-end encrypted VPN (Virtual Private Network) client connection. To access the remote access service via DA, Trust devices must be setup with VPN access; this process is managed by ICT; See **Appendix 2** for information relating to this solution.

- Staff can request remote access via the ICT Self-Service portal. This will require budget holder approval before the solution will be installed on the users Trust Laptop.

Remote Access via Remote Desktop

- Remote Desktop is a virtual Trust PC running in the cloud with the same setup and standard applications as a normal Trust PC or laptop enables staff to access their home and shared drives and their usual applications such as Rio, NHS.net, ESR, BigHand etc. from a non-Trust device.
- Staff can request Remote Desktop form via the ICT Self-Service portal. This will require budget holder approval.

3.1.1. Access to remote access solutions from outside UK is not permitted without approval from ICT. If access is required outside of the UK users must contact the ICT Service Desk

3.1.2. All staff are responsible for the security of information when using the remote access solution and are required to read the following Trust policies and guidelines:

- IG 02 ICT Policy
- IG 01 Confidentiality Policy
- IG 05 Information Governance Assurance Policy
- BSMHFT Safe Haven Guidelines.

3.1.3. The Trust remote access solution (DA) can only be installed on Trust devices.

3.1.4. Staff/users must report to the Trust immediately should there be loss, theft or damage to Trust ICT equipment or the loss of confidential information.

3.1.5. Staff/users must never disclose their network username and/or password Users should be vigilant when entering their password in a public place.

3.1.6. Wilful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

3.1.7. Members of staff who use remote access systems are responsible for safeguarding the equipment and confidential information at all times, for example, their work environment and when travelling.

3.1.8. Printing poses a risk to the Trust in that it may take place in a public or non-Trust location, and printed information could be inadvertently disclosed to those who have no need/ right to see it. It is therefore vitally important that if information is printed using this solution the user will:

- Ensure they are aware which printer the information will be sent to prevent the loss of information.
- Collect printed information immediately, to prevent loss and unauthorised disclosure.
- Secure the print copies as appropriate, to ensure confidentiality is retained at all times.

- Only print information where there is a clear need. If the printing can wait until staff are on Trust premises, this will always be the preferred option.
- If confidential printed information is lost report this as an IG incident immediately.
- The user is individually responsible for the security of information they print and must ensure its security at all times. If the user wished to dispose of printed information this must be carried out in a secure manner in line with Trust Policy

3.2 Remote Access for Third Party

The Trust currently operates a remote access solution for third party organisations.

3.2.1 All 3rd party organisations remote system access must be approved by the appropriate Trusts System Information Asset Owner via the ICT request for Change Process and by following approved BSMHFT processes.

4. Responsibilities

The table below defines responsibilities relevant to this policy:

Post(s)	Responsibilities	Ref
All Staff	All Trust staff should be aware of policies, such as Confidentiality Policy, ICT Policy and Information Governance Assurance policy that state clearly the appropriate way for handling, viewing and storing of data. Staff must be aware of the Safe Haven Guidelines that provides a clear understanding of the environment that the information should be used and that staff should always be aware of the problems that exist within that environment. Associated documents and related policies should be read in conjunction with and prior to signing the agreements attached to this document. All staff/ users must ensure they are familiar with the content of this document if they are working remotely. Staff/users must comply with all conditions including confidentiality, data protection, Health and Safety, working hours etc. Staff/users must never disclose their network username and password to anyone. Users	

	should be vigilant when entering their password in a public place. Staff/users must report to the Trust immediately should there be loss, theft or damage to Trust ICT equipment or the loss of confidential information. Staff/users must abide by the rules of all Trust policies which are connected to the use of information. Staff/users must manage the physical security of all equipment used to remotely access Trust systems. Staff working from home will be required to provide their own Internet connectivity.	
Staff with Remote Working DA	Staff working from home or third party (non-Trust) site will require access to a device with Internet connectivity.	
Staff with Remote Desktop	Staff working from home or third party (non-Trust) site will require access to a device with Internet connectivity. Staff working from home will be required to provide and maintain their own device.	
Policy Lead	The policy lead must ensure that ICT maintains this policy, standards and procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks. Ensures that ICT provides clear authorisation for all remote access users and the level of access provided. Ensures that ICT monitor remote access systems and report any misuse to line managers.	
ICT	ICT is responsible for: ICT will maintain the standards and procedures for remote access to ensure that risks are identified and appropriate controls are implemented to mitigate those risks. ICT will provide clear authorisation for all remote access users and the level of access required. ICT will monitor performance of remote access solutions.	

	ICT will monitor the remote access solution for inappropriate user access and report any misuse to line managers. ICT action Remote Access requests in a timely manner.	
ICT - Remote Working DA	ICT is responsible for the maintenance and support of the Trust device ICT do not provide support for users home or third party internet connectivity.	
ICT - Remote Desktop	ICT provide support for the Remote Desktop infrastructure within the Trust. ICT do not provide support for end user own device. ICT do not provide support for end user own Internet connectivity. ICT will not provide replacement or temporary devices in the event of user device failure.	
Third Party Organisations	Third party organisations must follow the agreed remote access process.	

5. Development and Consultation process

<table>
<tr><th colspan="3">Consultation Summary</th></tr>
<tr><td colspan="2"><b>Date policy issued for consultation</b></td><td>January 2021</td></tr>
<tr><td colspan="2"><b>Number of versions produced for consultation</b></td><td>1</td></tr>
<tr><td colspan="2"><b>Committees / meetings where policy formally discussed</b></td><td>Date(s)</td></tr>
<tr><td colspan="2"><b>Information Security Assurance Group</b></td><td></td></tr>
<tr><td colspan="2"><b>PDMG</b></td><td>March 2021</td></tr>
<tr><td><b>Where received</b></td><td><b>Summary of feedback</b></td><td><b>Actions / Response</b></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

6. Reference documents

None

7. Bibliography:

None

8. Glossary

Remote Access Solution	The physical equipment and network used to access the trust systems from outside
ICT	Information, Communication and Technology
VPN	Virtual Private Network
DA	Microsoft Direct Access solution

9. Audit and assurance consisting of:

Element to be monitored	Lead	Tool	Frequency	Reporting Arrangements
Number of Security Breaches	Head of ICT	ICT Service Delivery System	Monthly	ICT Managers Meeting ISAG Meeting
System Reports	Remote Desktop and Direct Access (DA) Lead	Remote Desktop System Reports DA System Reports	Monthly	Service Delivery Team Meeting

10. Appendix 1 – Equality Analysis Screening Form

A word version of the Equality Analysis Screening form is available on the HR support pages on Connect via this link.

Title of Proposal	**ICT Remote Access**		
Person Completing this proposal	**Mark Thornton**	**Role or title**	**ICT Technical Specialist**
Division	**Corporate**	**Service Area**	**ICT**
Date Started	**05/10/2020**	**Date completed**	**05/10/2020**
Main purpose and aims of the proposal and how it fits in with the wider strategic aims and objectives of the organisation.			
Who will benefit from the proposal?			
Staff with BSMHFT remote network access			

Impacts on different Personal Protected Characteristics – *Helpful Questions:*	
Does this proposal promote equality of opportunity? *Eliminate discrimination?* *Eliminate harassment?* *Eliminate victimisation?*	*Promote good community relations?* *Promote positive attitudes towards disabled people?* *Consider more favourable treatment of disabled people?* *Promote involvement and consultation?* *Protect and promote human rights?*

Please click in the relevant impact box or leave blank if you feel there is no particular impact.				
Personal Protected Characteristic	**No/Minimum Impact**	**Negative Impact**	**Positive Impact**	**Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.**
Age				
Including children and people over 65 Is it easy for someone of any age to find out about your service or access your proposal? Are you able to justify the legal or lawful reasons when your service excludes certain age groups				
Disability				
Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families?				

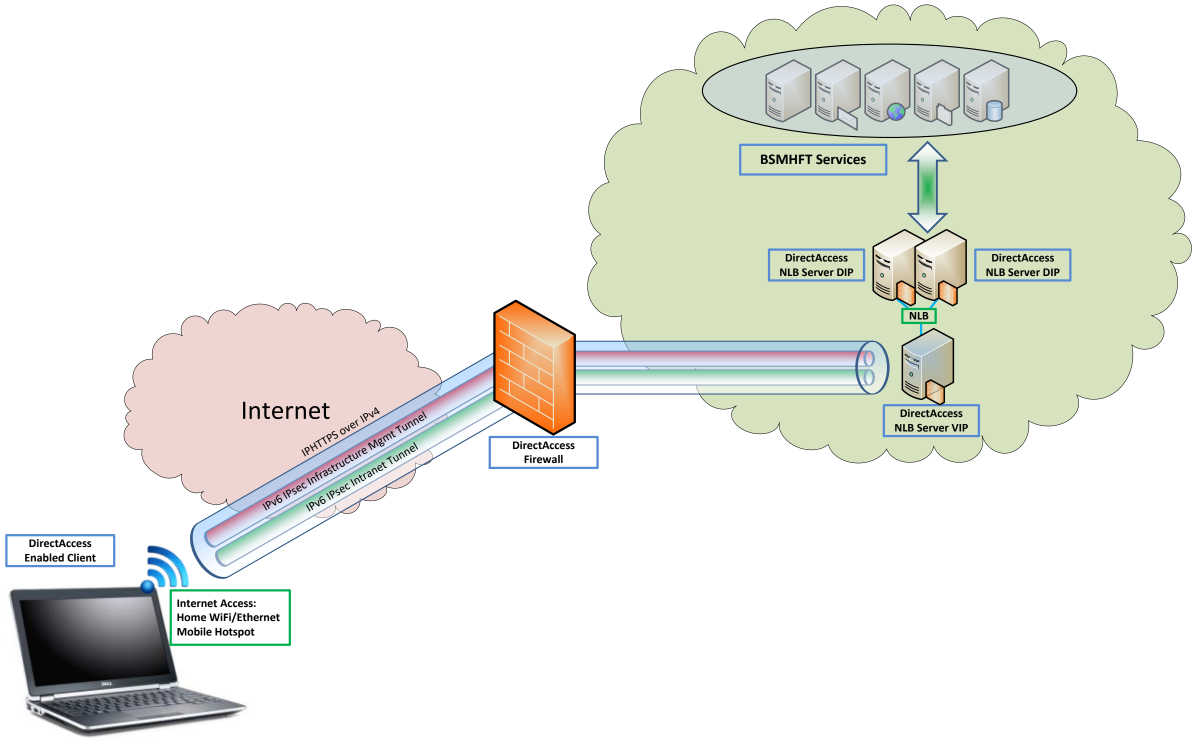
Gender				
This can include male and female or someone who has completed the gender reassignment process from one sex to another Do you have flexible access arrangements for either sex? Is it easier for either men or women to access your proposal?				
Marriage or Civil Partnerships				
People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?				
Pregnancy or Maternity				
This includes women having a baby and women just after they have had a baby Does your service accommodate the needs of expectant and post natal mothers both as staff and service users? Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity?				
Race or Ethnicity				
Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees What training does staff have to respond to the cultural needs of different ethnic groups? What arrangements are in place to communicate with people who do not have English as a first language?				
Religion or Belief				
Including humanists and non-believers Is there easy access to a prayer or quiet room to your service delivery area? When organising events – Do you take necessary steps to make sure that spiritual requirements are met?				
Sexual Orientation				
Including gay men, lesbians and bisexual people Does your service use visual images that could be people from any background or are the images mainly heterosexual couples? Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea?				
Transgender or Gender Reassignment				
This will include people who are in the process of or in a care pathway changing from one gender to another Have you considered the possible needs of transgender staff and service users in the development of your proposal or service?				
Human Rights				

Affecting someone’s right to Life, Dignity and Respect? Caring for other people or protecting them from danger? The detention of an individual inadvertently or placing someone in a humiliating situation or position?				
If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)				
	Yes	**No**		
What do you consider the level of negative impact to be?	**High Impact**	**Medium Impact**	**Low Impact**	**No Impact**
				X
If the impact could be discriminatory in law, please contact the **Equality and Diversity Lead** immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required. If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the **Equality and Diversity Lead** before proceeding. If the proposal does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the **Equality and Diversity Lead.**				
Action Planning:				
How could you minimise or remove any negative impact identified even if this is of low significance?				
How will any impact or planned actions be monitored and reviewed?				
How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.				
Please save and keep one copy and then send a copy with a copy of the proposal to the Senior Equality and Diversity Lead at hr.support@bsmhft.nhs.uk. The results will then be published on the Trust’s website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis.				

11. Appendix 2 – Direct Access

Microsoft Direct Access allows connectivity for remote users to the BSMHFT network without the need for traditional VPN connections.

- Staff access on a non-Trust site will require access to a Trust device with DA installed and Internet connectivity
- ICT is responsible for the support and maintenance of the Trust device
- ICT are not responsible to the home or third party internet connections.


BSMHFT Services
DirectAccess NLB Server DIP
DirectAccess NLB Server DIP
NLB
DirectAccess NLB Server VIP
Internet
IPHTTPS over IPv4
IPv6 IPsec Infrastructure Mgmt Tunnel
IPv6 IPsec Intranet Tunnel
DirectAccess Firewall
DirectAccess Enabled Client
Internet Access: Home WiFi/Ethernet Mobile Hotspot

12. Appendix 3 – Remote Desktop Solution

What is a Windows Virtual Desktop (WVD)?
WVD is a remote desktop solution which facilitates secure user access to Trust applications as if they were running locally. Providing staff with secure access to everything they need from virtually any device, without requiring specific Trust hardware.

Criteria:

- Staff must only access Remote Desktop via an updated, supported and secure device
- The Remote Desktop solution cannot be used at a Trust site.

Applications Available via Remote Desktop:

- Rio
- NHSmail
- BigHand
- Microsoft Office
- Other web-based systems accessible via a Trust Desktop PC.

BSMHFT ICT Support and Responsibilities:

- ICT only provide support the Remote Desktop infrastructure within the Trust
- ICT do not provide support for end user own device
- ICT do not provide support for end user own Internet connectivity issues
- ICT will not provide replacement device in the event of user device failure.
- ICT will not provide a temporary device.

Staff Requirements:

- Staff access on a non-Trust site will require access to a device with Internet connectivity
- Staff access from home will be required to provide and maintain their own device
- Staff access from home will be required to provide and maintain their own Internet connectivity
- Staff will be responsible for replacing their own device in the event of device failure.

Staff wishing to request access to Remote Desktop and for up to date licencing costs should go to the ICT Self-Service portal on Connect.

13. Appendix 4 – Third Party Access Process

All Third Party Access is managed by the ICT Service Delivery team.

- **ICT Network Access Form** – BSMHFT staff access to the network
- **ICT 3rd Party Network Access Form** – Third party staff access to network
- Infrastructure, Support and Maintenance Process (HSCN)
- **Information Sharing Protocol** (IG Document)
- **SOP10 Third Party Access to Servers & Applications**