St Hugh's School

Remote Access Policy

Remote Access Policy v1.0
17/11/15

1. **Introduction**

1.1 Advancement in technologies can now allow organisations to create and deploy systems that allow mobile networking and remote access for all or specific employees. Benefits include support of flexible working (flexi time), 24/7 environments and the ability to facilitate a greater efficiency and effective use of time.

1.2 With this advancement and thus rise in remote access to the corporate network, the risk to digitised data that traverses the World Wide Web greatly increases. Risks include plagiarism, theft, and data corruption or simply lost data/information.

1.3 Realisation of the above risks through the misuse and non-compliance of remote access procedures places remote access users in breach of moral, ethical, legislative or contractual obligations.

1.4 St Hugh's School and its IT services, support secure, safe, accessible and available remote access and mobile working through its systems and policies, through the provision of essential technical controls and through raising user awareness and encouraging good working practices.

1.5 Users with remote access permissions must be aware of procedures and responsible ethical practices.

1.6 **Definitions**

1.6.1 **Remote Access** - accessing the St Hugh's network from outside of the St Hugh's premises via a different network through the use of a configured St Hugh's laptop.

1.6.2 **Mobile Working** – performing tasks on the network, from connectivity outside of the network (i.e. the creation, storage, processing and transport or transfer of data/ information) as an employee of St Hugh' School.

2. Scope & limitations

2.1 The St Hugh's School remote access policy applies to all remotely accessible systems and authorised remote access users and data that is controlled by the St Hugh's School.

2.2 St Hugh's School does not make provision for all its systems and services to be made available remotely to all users with remote access permission.

2.3 With regard to availability and speed of remote access services, it should be borne in mind that these may be reliant on 3rd party factors such as the users Internet Service Provider connectivity and/or domestic networking hardware such as routers/switches.

3. Available Remote Services

3.1 The privilege of remote access is at the discretion of the Head Teacher and access is dependent on their current network and system permissions and access rights

3.2 Senior Leadership Team has access to the following:-

- Clerical shared area
- SLT shared area
- Staff shared area
- Students shared area
- Media shared area
- Curriculum shared area
- Student shared area
- Teaching School shared area

3.3 Clerical staff has access to the following:-

- Clerical shared area
- Staff shared area
- Students shared area
- Media shared area
- Curriculum shared area
- Student shared area

3.4 External Users (Local Authority)

3.4.1 The default situation for external users (typically the CMISS team) is they are given **No** ad-hoc remote access to St Hugh's systems. If remote access is required, agreed dates and times will be set and the relevant user account will be enabled (in Active Directory) and promptly disabled once the work is complete.

4. Methods of Remotely Access

4.1 Remote access to the St Hugh's School network is provided by Microsoft's built in Remote Desktop Connection application using the North Lincolnshire's remote desktop gateway.

4.2 Remote access users must sign in via the gateway using a valid St Hugh's Active Directory username and password.

5. Remote Access for 3rd Party and Systems Suppliers

5.1 If possible, recently purchased software that requires external connectivity via a secured line should be provided onsite, as opposed to being performed using remote access. If this is not possible, remote access that allow installations should be monitored until the completion of the installation and the remote session has ended.

5.2 Existing systems suppliers remotely accessing St Hugh's systems services must contact the school and inform of the changes that are to be made along with times and dates of the required remote access session.

5.3 User accounts for system suppliers and support should be kept disabled when not in use.

6. User responsibilities and good working practices

6.1 The primary responsibilities of employees of St Hugh's School and other users that remote into the St Hugh's network are to:

i. Know what information they are accessing, using or transferring

ii. Understand and adhere to contractual, ethical or other requirements attached to the information and pertinent to St Hugh's School policies and procedures.

iii. Users are responsible for following correct procedures when logging out of the remote session

6.2 Responsibilities for data/ information accessed and/ or processed during mobile working

i. Confidential data/information should not be created, stored or processed on privately owned computers.

ii. 3rd party devices should not be considered or assumed to be secure and the use of such devices for storing documents or other work related to St Hugh's School is discouraged. St Hugh's systems that have been allocated to staff do have strong controls and are configured to protect the integrity of the data.

iii. Appropriate precautions and good practice should be followed for all data and information that has been edited, created and/or saved on mobile or home devices or other forms of media.

6.3 Security of privately owned computers and other mobile working devices

6.3.1 If users are using their own personal systems or other mobile devices to carry out work for St Hugh's School then the following points should be noted and followed:

- Keep abreast of current security threats and issues for their device type, whether that is related to hardware or software
- Maintain safe web-surfing practice.
- Each device is equipped with up-to-date anti-virus software and other security software such as malware and a configured firewall.
- They perform critical operating System updates as soon as they become available.
- They practice good password hey utilise other cryptographic (password) controls as appropriate.
- They do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to their role.
- Mobile devices are not left unattended or data that is deemed confidential data is left visible on the screen in public areas.

- If the system has suffered loss of data, corruption of data or any other issues that may impact the network or other systems at St Hugh's is reported as soon as possible to the SLT and IT support at St Hugh's School.

6.4 Security of St Hugh's owned computers or other mobile devices

6.4.1 If users are utilising St Hugh's owned systems or other forms of mobile device to perform work for St Hugh's then it is considered secure for remote access. Users should still:

- Keep abreast of current security threats and issues for their device type, whether that is related to hardware or software.
- Return the device to IT support for system faults, system security updates and patches or any other security related issues.
- Maintain safe web-surfing practice.
- Regularly back up work that has been stored locally on their specific device.
- Passwords are changed regularly and follow St Hugh's password policy guidelines.
- Mobile devices are not left unattended or data that is deemed confidential data is left visible on the screen in public areas.
- They do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to their role.

7. Return of assets to St Hugh's School

7.1 All St Hugh's owned systems and other devices and information/data must be returned to St Hugh's upon termination of employment or contract.

7.2 St Hugh's systems should be returned prior to the user leaving for critical system updates or re-imaging.

7.3 Before returning the system, users should remove their own personal data from the system.

8. Removal of Remote Access Rights

8.1 Access rights to for remote access may be changed or removed by St Hugh's from any authorised/unauthorised user at any time if a breach of the conditions of use has been performed or that user's access is compromising the confidentiality, integrity and/or availability of the St Hugh's systems or services.

8.2 The remote access rights of all employees and third party users shall be removed upon termination of employment, contract, or agreement.