



SMITHDON HIGH SCHOOL

HUNSTANTON

ICT SECURITY POLICY

**Re-adopted by Local Governing Body
February 2022**

Work hard, be kind and smile

Concerns and Risks

Any removable storage used from home may contain a virus.

Accessing the Internet and downloading could contain a virus.

Users staying logged on and leaving machines could allow access to files by unauthorised person(s).

Disks containing confidential records left in machines after use.

Unauthorised user(s) obtaining staff passwords.

Users installing unauthorised or unlicensed software.

Data being changed or deleted by unauthorised user(s).

Users unaware of the legal responsibilities when using software or when recording data.

Security Responsibilities/Procedures

Virus checking

Students are actively encouraged to transfer work from home. However students in Years 7 to 11 do not have access to removable media and are encouraged to use the school's email system to complete this task. If removable media from home is used the student should take the media to the ICT Support Team for the work to be transferred. All PC's in the school have up to date anti-virus software and any removable media is automatically scanned.

Our connection to the Internet is via BT which includes a secure connection by a filtering system and virus checking.

The school's email system is provided by Google and includes virus checking.

General procedures

Logging on and logging off

All staff will need to log on using their own username and a password. Staff should ensure that during log on procedure they do not allow others to access their password. Passwords should not be written down. If passwords are obtained by others, they should be changed immediately. Once a session is ended users should log off; machines should not be left unattended and logged in. If a member of staff leaves a machine, it should be locked.

Administration Files

Staff will have a security level, which will allow access only to appropriate areas of the Management Information System (SIMS.et). If the appropriate level has not been set staff should inform the ICT Systems Manager. After log on staff have access to a drive labelled Q: Staff Documents, which only staff can access. Staff files should be stored in a Google shared drive.

Use of removable storage

If removable storage is used to copy details from school to home the appropriate levels of confidentiality and security are to be employed. Users should ensure that removable storage items are not left in PCs after use or where unauthorised users have access to it.

Access From Home

Access to the Smithdon network is provided by a secure VPN connection using L2TP/IPsec with pre-shared key protocol, using AES 256-bit encryption. Each staff member is given a unique username and a complex password to prevent any password guessing from an unknown source.

Curriculum

Staff can create files that students will need to access by storing work on the shared drive, T: in the appropriate subject folder. Students will also be able to place files for staff to access on this drive. Periodic cleaning of this drive will take place with files that have not been accessed for a long period of time being deleted, so staff should delete files as soon as they are no longer required; files left on this drive should be a copy. Any files/folders with inappropriate names will be deleted. Photographs of students should not be placed on the T drive.

Legal requirements

Users should make themselves aware of the legal requirements when using computerised records. Please refer to the section on Data Protection.

System for reporting security incidents

Any breaches of security should be dealt with immediately and reported to the **ICT Systems Manager**.

Backing up the system

Full system backups are performed weekly on a Friday to a dedicated backup server using the popular Veritas Backup Exec software; additionally, a full backup is also taken and stored on a Synology NAS device.

Once a month the onsite Senior ICT Technician perform a manual backup of all staff and student's documents to which are backed up to a removal hard drive. To which is then stored away for safe keeping at the end of the month when a replacement hard drive is then added for the following month, a total of 12 months' data is kept in storage.

Software Policy

Legal requirements

Only software with sufficient licenses will be installed on the network.

Consistent software

The school has adopted Microsoft Office and Google Suite as the main software to be used.

Installing new software

Software to be installed on the network is to be installed by the ICT Systems Manager due to the level of access required to install software and the necessity for the ICT Systems Manager to be aware of all software that is accessed on the network.

Data Protection Principles

Staff should ensure they are aware that:

Registered data users must comply with the Data Protection Principles in relation to the personal data they hold. Broadly they state that personal data shall:

- Be obtained and processed fairly and lawfully.
- Be held only for lawful purposes which are described in the register entry.
- Be used or disclosed only for those or compatible purposes.
- Be adequate, relevant and not excessive in relation to the purpose for which they are held.
- Be accurate and, where necessary, kept up to date.
- Be held no longer than is necessary for the purpose for which they are held.
- Be able to allow individuals to access information held about them and where appropriate, correct or erase it.
- Be surrounded by proper security.

The Principles also provide for individuals to have access to data held about themselves and, where appropriate, to have the data corrected or deleted.

To enforce compliance with the Principles, the Registrar can serve three types of notice:

- An enforcement notice, requiring the data user to take specified action to comply with the particular Principle. Failure to comply with the notice would be a criminal offence.
- A de-registration notice, cancelling the whole or part of a data user's register entry. It would then be a criminal offence for the data user to continue to treat the personal data subject to the notice as though they were still registered in the same way.
- A transfer prohibition notice, preventing the data user from transferring personal data overseas if the Registrar is satisfied that the transfer is likely to lead to a Principle being broken. Failure to comply with the notice would be a criminal offence.