BRECON HIGH SCHOOL

YSGOL UWCHRADD ABERHONDDU

ICT Technical Security Policy

Author	**Andrew James**
Agreed By	**Governors on 22/05/18**
Review	**05/2019**

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Brecon High School is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- No user should be able to access another's files (other than that allowed for monitoring purposes within the school policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- There is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the overall responsibility of the Head Teacher, with Day to day responsibility filtered to Brecon High Schools ICT Systems Manager and School Business Manager.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- There will be Annual reviews and audits of the safety and security of school/college network.
- Servers are stored within a locked room, within the ICT Managers Office, access to which is restricted by key code.
- All users will have clearly defined access rights to school network. Details of the access rights available to groups of users will be recorded by the ICT Systems manager and will be reviewed, at least annually, by the online safety group.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (see password section below).
- The ICT Systems Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Mobile devices are only permitted to connect to the school wireless system via the individuals personal username / password.
- The ICT Systems Manager regularly monitors and records the activity of users on the school network Via and users are made aware of this in the acceptable use Policy.

- Impero classroom Monitor is in place in the schools IT rooms to be used by staff to control workstations and view users activity
- Users are required to report any breach of security or usage to the ICT Systems Manager immediately. All users of the schools technical system are required to sign an acceptable usage policy (See acceptable usage policy below), Pupils are required to sign on every login, and staff and visitors once per month.
- All users are forbidden from downloading executable files and the installation of programmes on school devices (See acceptable usage policy below)
- All staff and Pupils are allowed to use removable storage devises within the school System, all staff must ensure that the devices are encrypted as per the schools GDPR Policy, and both staff and pupils must ensure that removable devices are virus scanned when connected to the school system.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc. This is via ESET.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

Policy Statements:

- All users will have clearly defined access rights to school network and devices. Details of the access rights available to groups of users will be recorded by the ICT Systems Manager and will be reviewed, at least annually, by the online safety group.
- All school networks and systems are protected by secure passwords that are regularly changed
- The "Emergency Administrator" passwords for the school systems is kept in a sealed envelope in the schools safe
- Passwords for new users, and replacement passwords for existing users will be allocated by the ICT Systems Manager.
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals – as described in the passwords section below.
- Requests for password changes will only be carried out by the ICT System Manager with the presence of the account holder.

Passwords:

- All staff and Pupil users will be provided with a username and password by the ICT Systems Manager, who will keep an up to date record of users and their usernames.
- Passwords will be a minimum of 7 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- The account will be locked after 5 invalid login attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)

- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school/college
- Passwords are required to be changed every 120 days.
- The last 2 passwords cannot be re-used.
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school/college

Acceptable Use Policy

Policy: Statements

It is appropriate for students to be allowed a great deal of freedom in using ICT for study. With freedom comes responsibility. If material is considered to be unacceptable by the school when presented in a book, magazine, video, audio tape or spoken form, then it is not acceptable on the ICT network.

We expect ALL ICT users to take responsibility in the following ways:

Not to access or even try to access any material which is:

- Violent or that which glorifies violence
- Criminal, terrorist or glorified criminal activity (including drug abuse)
- Racist or designed to incite racial hatred
- Of extreme political opinion
- Pornographic or with otherwise unsuitable sexual content
- Crude, profane or with otherwise unsuitable language
- Blasphemous or mocking of religious and moral beliefs and values
- Offensive in the normal context of a Christian school
- In breach of the law, including copyright law, data protection, and computer misuse
- Belongs to other users of ICT systems and which they do not have explicit permission to use

- Not to search for, or use websites that bypass the school's Internet filtering
- Not to access social networking sites during, lessons or break times.
- Not to download or even try to download any software without the explicit permission of a member of the ICT department.
- Not to attempt to install unauthorised and unlicensed software
- To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number, on social networking sites or e-mails to strangers
- Not to use other people's user ID or password, even with their permission
- Not to interfere with or cause malicious damage to the ICT resources and facilities

To report any breach (deliberate or accidental) of this policy to the ICT Manager immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Any use of the ICT may be monitored and recorded, including the contents of e-mail messages, by our security system "Impero” to ensure that this policy is followed.

Brecon High School reserves the right to access all material stored on its ICT system, including that held in personal areas of staff and pupil accounts, including email mailboxes, for purposes of ensuring Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety.

Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the ICT facilities. Brecon High School will act strongly against anyone whose use of ICT risks bringing the school into disrepute or risk the proper work of other users. Persistent offenders will be denied access to the ICT facilities - on a permanent basis.