Bebington High
Sports College

School Technical Security Policy

January 2017

Contents

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the infrastructure / 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's 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 Network Manager has responsibility for the security of the network, subject to review, at least annually, by the Online Safety Group.

Policy statements

The school is 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. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and

data. All equipment is contained with a room which is locked when unattended by technical Support or ICT staff.

- The Network Manager is responsible for the management of technical security in accordance with the agreed policy.
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager and Technical Support staff and will be reviewed, at least annually, by the Online Safety Group.
- Users will be 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.
- The Network 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 device security and management procedures are in place for school provided devices. All devices are security marked and appropriate virus checking software is installed prior to usage.
- School technical support staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users' activity where such tools are available.
- Users should report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician.
- Temporary access to the computer systems may be provided to allow access to the system for of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system. These accounts should be disabled/deleted when no longer required.
- The downloading and installation of executable files may be undertaken by staff users with the agreement of Technical Support. Students should not download executable files and permissions will be set to avoid this.

- Removable media (e.g. memory sticks / CDs / DVDs) may be utilised by users on school devices and will be subject to virus checking on loading.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Group.
- All school networks and systems will be protected by secure passwords that are regularly changed.
- The "administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- 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.
- Passwords for new users and replacement passwords for existing users will be allocated by Technical Support and ICT staff.
- Users will change their passwords at regular intervals.
- Where passwords are set or changed manually, requests for password changes should be authenticated to ensure that the new password is only passed to the genuine user.

Staff Passwords

- All staff users will be provided with a username and password by Technical Support staff who will keep an up to date record of users and their usernames.
- the password should be a minimum of 8 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 should be "locked out" following six successive incorrect log-on 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
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous passwords created by the same user.

Student Passwords

- All users will be provided with a username and password by Technical Support staff who will keep an up to date record of users and their usernames.
- Students will be taught the importance of password security

Training / Awareness

.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in lessons as part of the e-safety lessons in Y7
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The Technical Support staff will ensure that full electronic records are kept of:

- User log-ins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Filters will be utilised to manage Internet access:

- Filtering service from the LA are implemented using the recommended lists for schools.
- An additional level of filtering is provided via the implementation of Impero software using the Dfee recommended list. Additional sites may be added to this list in accordance with school procedures. Sites will not be removed from this filter in accordance with Dfee recommendations.
- Differentiated filtering is implemented for students and staff.
- User monitoring systems, using the Impero software, will be used to supplement the filtering system. A report detailing Internet sites accessed, using a list of identified sites and search words is created for inspection to identify inappropriate Internet activity.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems. To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must be logged by the Technical Support staff. In addition they should:

- be logged in change control logs
- be reported to a second responsible person (Technical Support Manager) on a weekly basis in the form of an audit of the change control logs
- be reported to the Online Safety Group every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Online Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the LA
- In addition the school manages its own filtering service utilising the Prevent recommended lists
- The school has provided enhanced user-level filtering through the use of the Impero filtering programme.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or Online Safety Coordinator.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education, Training and Awareness

Students will be made aware of the importance of filtering systems through the online safety education programme during e-safety lessons delivered as part of the curriculum They will also be made aware of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety information available on the school website.

Changes to the Filtering System

These changes may be made only in accordance with the following conditions:

- requests for changes to the filtering should in the first instance be made to the Technical Support staff.
- There should be strong educational reasons for changes that are agreed if the filters are to be removed for sites. This should only occur in highly exceptional circumstances and with the agreement of the Online Safety Coordinator.

- Liable to the Online review group.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to Technical Support, who will decide whether to make school level changes.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows utilising the Impero software access logging and reporting software.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Online Safety Coordinator
- Online Safety Group
- Online Safety Governor
- Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.