Bennerley Fields School

Technical Security Policy

Version	Date	Minute Number
1 - Date Approved	16.12.2014	16.2.13
1.1	07.11.2016	10.9
1.1	11.12.2017	19.15
Review Requirement : 1 Year		

Bennerley Fields School

Technical Security Policy

(including filtering and passwords)

Agreed by Computing and e-Safety Committee on: 11th Dec 2014

Approved by Governors on:16th December 2014

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 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's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- 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 responsibility of Technical Staff and the School Business Manager.

Technical Security

Policy statements

The school will be responsible for ensuring that the school 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 will 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.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- 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 School Business Manager and will be reviewed, at least annually, by the e-Safety Committee.
- 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.
- The School Business Manager is responsible for ensuring that software licences logs are up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- An appropriate system is in place for users to report any actual/potential technical incident to the School Business Manager.
- An agreed policy is in place for the provision of temporary access of “guests” onto the school system.
- Access restrictions prevent the downloading of executable files and the installation of programmes on school devices by unauthorised users
- The following are described in the school’s Acceptable Use of the Internet and Electronic Communication policy:
  - the provision of temporary access of “guests” onto school systems.
  - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school devices that may be used out of school.
  - Access restrictions that stop unauthorised staff from downloading executable files and installing programmes on school devices.
  - the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices. 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.

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 School Business Manager and will be reviewed, at least annually, by the Computing/E-Safety Committee.
- 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 School Business Manager and kept in a secure place eg school safe.
- Passwords for new users, and replacement passwords for existing users will be allocated by the School Business Manager.
- All staff 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.
- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account
- Requests for password changes should be authenticated by the School Business Manager to ensure that the new password can only be passed to the genuine user.

Staff passwords

- All staff users will be provided with a username and password by the School Business Manager 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 three 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 (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

Pupil passwords

Use by pupils should always be supervised and members of staff should never allow pupils to use a device logged into the network/internet on their own log on. Schools should consider the implications of using whole class log-ons when providing access to applications which may be used outside school.

- All users at KS3 and above will be provided with a username and password by the School Business Manager who will keep an up to date record of users and their usernames.
- Users will be required to change their password once each academic year
- Pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

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

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

Pupils / students will be made aware of the school's password policy:

- in lessons

- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The School Business Manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- 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 e-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.

School will:

- allow flexibility for sites to be added or removed from the filtering list for their organisation.
- have differentiated filtering for different groups / ages of users

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the School Business 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 in change control logs
- be reported to a second responsible person (e-Safety Coordinator):
- be reported to the E-Safety Committee every half term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the School Business Manager 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, hardware 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 broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated. 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 Internet Service Provider (Wave9)
- The school has provided enhanced / differentiated user-level filtering through the use of Wave9's 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 other nominated senior leader).
- Mobile devices that access the school / academy 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 School Business Manager, in consultation with the e-Safety Coordinator if necessary. If the request is agreed this action will be recorded and logs of such actions shall be reviewed regularly by the Computing and eSafety Committee.

Education/Training/Awareness

Pupils / students will be made aware of the importance of filtering systems through the e-safety education programme.They will also be warned 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 e-safety awareness sessions/newsletter etc

Changes to the Filtering System

- users may email request changes to the School Business Manager with details of why the change is required
- the School Business Manager will authorise the change based on the guidelines set down in the e-Safety Policy.
- if necessary the e-Safety Coordinator will be consulted before changes to the filtering system are made

- all changes to the filter system will be logged by the School Business Manager and reviewed by the e-Safety Committee half-termly.

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 the School Business Manager who will decide whether to make school level changes (as above).

Audit/Reporting

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

- the second responsible person (e-Safety Coordinator)
- E-Safety Committee
- E-Safety Governor
- External Filtering provider/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.