Ravenshall

all different | all equal | all important

Technical Security Policy

November 2018

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 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 management of technical security will be the responsibility of the network manager and SLT.

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. 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 are kept in a locked rack cabinet**
- **Appropriate security measures are in place to protect the servers (Secure back up using Microsoft Server security, anti-virus software, UPS) , firewalls (Window Firewall), switches, wireless systems (Password protection), work stations, mobile devices (Management software) 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 from technical support company (MGL)**
- **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 / Technical Staff (or other person) and will be reviewed, at least annually, by the Online safety Committee (or other 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.

- Network manager/school business manager & technical staff are 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.*
- *School technical staff regularly monitor and record the activity of users on the school technical 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*
- *An appropriate system is in place (see escalation process document) for users to report any actual / potential technical incident to the Online safety Coordinator / Network Manager / Technician*
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system. Access will be approved by the network manager and the school technical will provide temporary access.
- *An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users*
- *An agreed policy (AUP) is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices* . All removable pen drives must be scanned before use. Staff members must use a school issued encrypted pen drive for sensitive data.
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc. ESET anti-virus is currently used.*
- *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 (or other person) and will be reviewed, at least annually, by the Online safety Committee (or other group).
- **All school networks and systems will be protected by secure passwords.**
- **The "master / administrator" passwords for the school systems, used by the technical staff are available to the *Headteacher* & Network manager and kept in a secure place**
- *Passwords for new users, and replacement passwords for existing users will be allocated by school technician which has been authorised by Network 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.

- *requests for password changes should be authenticated by the network 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 schools technician 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*
- *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 (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*
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous p*ast four passwords cannot be re-used* passwords created by the same user.
- 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

Student / pupil passwords

- KS1 Pupils- username no password
- Year 3 & 4 & 5 - generic Password issued by school
- **Year 6 + All users will be provided with a username and password**
- Students / pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

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

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

- in online safety lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (insert title) 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 online safety and acceptable

Responsibilities

The responsibility for the management of the school's filtering will be held by the DSL, supported by the 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 in change control logs**
- **be reported to a second responsible person** (headteacher)**:**
- *be reported to the Online safety Group regularly in the form of an audit of the change control logs*

All users have a responsibility to report immediately to network 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 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 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 Internet Service Provider*
- *The school has provided enhanced / differentiated user-level filtering through the use of the* Smooth wall *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 .*
- *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* and the network manager *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 / Awareness

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 awareness sessions / newsletter etc.

Changes to the Filtering System

- changes to the filtering must be requested to the network manager and then discussed with the technician
- Access to unavailable site for the purposes of teaching & learning must be requested to the network manager and then agreed with the headteacher.
- The computing / online safety co-ordinator, SMT will monitor any logs made to the filtering system.

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 online safety co-ordinator 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 termly, the technician will produce reports which have been requested by the SMT.*

Audit / Reporting

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

- *the second responsible person* (Head of School)
- *Online safety Group*
- *Online safety Governor / Governors committee*
- *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.

Further Guidance

The following is recommended:

NEN Technical guidance: http://www.nen.gov.uk/advice/266/nen-guidance-notes.html

Reviewed October 2019