West Exmoor Federation

Technical Security Policy

May 2016

West Exmoor Federation Technical Security Policy Template (including filtering and passwords)

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 federation will be responsible for ensuring that the federation 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
- the federation will ensure that our managed service provides (Scomis/SWGfL/Tiger Technologies) carry out all the online safety measures that might otherwise be carried out by the *federation* (as stated below).

Responsibilities

The management of technical security will be the responsibility of the Executive Headteacher.

Technical Security - Policy statements

The federation will be responsible for ensuring that the federation's 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:

- The federation's technical systems will be managed in ways that ensure that the federation meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of the federation's 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 federation's 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 the federation's technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed at least annually.

- Users will be made responsible for the security of their username and password and 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 Executive Headteacher 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 (Inadequate licencing could cause the federation to breach the Copyright Act which could result in fines or unexpected licensing costs);
- Mobile device security and management procedures are in place, eg, device MAC addresses have to be resisted with Scomis before being able to access the network.
- Federation 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 for users to report any actual / potential technical incident to the Executive Headteacher.
- Staff should not make personal use of federation devices that may be used out of school and members of their family should not be permitted access to any device.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Such media should be avoided whenever possible but when used must be encrypted and deleted as soon as the necessary data has been transferred.
- 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 - Policy Statements

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

- All users will have clearly defined access rights to federation 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;
- All federation networks and systems will be protected by secure passwords that are regularly changed;
- The "master / administrator" passwords for the federation systems, used by the technical staff must also be available to the Executive Headteacher or other nominated senior leader and kept in a secure place eg school safe.;
- All users (adults and young people) will have responsibility for the security of their username and password and 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 Scomis and/or Tiger Technologies. Any changes carried out must be notified to the manager of the password security policy;
- Users will change their passwords at regular intervals;

- Where passwords are set / changed manually 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 Tiger Technologies 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
- 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
- Passwords should be changed at least every 60 to 90 days
- Passwords should not re-used for 6 months and be significantly different from previous passwords created by the same user.

Pupil Passwords

- All users (at KS2 and above) will be provided with a username and password by Tiger Technologies who will keep an up to date record of users and their usernames.
- 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 federation's password policy:

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

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

- in lessons with regular reminders when using IT;
- through termly internet/IT safety sessions.

Audit / Monitoring / Reporting / Review

The responsible person (Network Manager) will ensure that full records are kept of:

- User Ids and requests for password changes
- 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 federation has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this federation. The federation will mainly use the SWGfL without change. However, specific requests can be made to the Executive Headteacher to enable otherwise blocked sites. If approved, the Executive Headteacher will request that SWGfL unblocked agree sites.

Responsibilities

The responsibility for the management of the federation's filtering policy will be held by SWGfL. They will manage the federation 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 federation filtering service must be logged in change control logs.

All users have a responsibility to report immediately to the Executive Headteacher any infringements of the federation'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 federation. 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 federation 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. Personal mobile devices are not allowed internet access through the school network.

- The federation supports the managed filtering service provided by the Internet Service Provider (SWGfL).
- 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 federation internet connection 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 Executive Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme run by the federation. 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 online safety awareness sessions / newsletter etc.

Changes to the Filtering System

Requests to make changes to the filtering system should be made to the Executive Headteacher. Such a request will only be approved if there are strong educational reasons for the proposed changes. If approved a request will be made to the SWGfL where the change will be recorded. 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 Executive Headteacher will decide whether to request federation level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The federation 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.

Audit / Reporting

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

- Safeguarding 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.

Further Guidance

Further recommended guidance can be found within the following documents:
Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).
Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."
In response UKSIC produced guidance on – information on "Appropriate Filtering"
NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/
Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx