September 2023

Audley Infant School

Technical Security Policy Including Filtering and Monitoring

SWGFL

Audley Infant School

School Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures but also on appropriate policies and procedures and 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 the right to 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 processes
- logs are maintained of access by users and 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 an impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Imraan Rawat

Technical Security

Policy statements

The school will be responsible for ensuring that its 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, workstations, 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 assigned to appropriate and well-trained staff, school have an SLA with Computerserve to manage the school system and network**
- **all users will have clearly defined access rights to school technical systems.**
- **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 details and must immediately report any suspicion or evidence that there has been a breach of security**
- Imraan Rawat/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
- mobile device security and management procedures are in place- devices access the network only with agreement from the Headteacher.

Audley Infant School

School Technical Security Policy (including filtering and passwords)

- Local authority provides a report that regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. Fortinet is the filtering software for the network internet.
- An IT reporting ticket system is in place for users to report any actual/potential technical incident to the network manager/technician
- The provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school's systems is managed by the IT Technician and is with agreement from the Headteacher
- The downloading of executable files and the installation of programmes on school devices is managed by the IT technician or with agreement from the Headteacher
- School devices that may be used out of school must not be used for personal use by school users or their families unless agreed with the Headteacher
- an agreed policy is in place which allows users to use removable media for education. (see online safety policy)
- the school's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, Trojans etc. (Sophos)
- 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 learning platforms).

Further guidance can be found from the National Cyber Security Centre and SWGfL "Why password security is important"

Policy Statements:

- **These statements apply to all users.**
- **All school networks and systems will be protected by secure passwords.**
- **All users 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 group (or other group).**
- **All users (adults and learners) 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 must not be shared with anyone.
- All users will be provided with a username and password by IT Technician, Imraan Rawat, who will keep an up-to-date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack.

Password length trumps any other special requirements such as uppercase/lowercase letters, numbers and special characters. Passwords should be easy to remember, but difficult to guess or crack.

- 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 must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on the first login to the system
- Passwords should not be set to expire as long as they comply with the above but should be unique to each service the user logs into.

Learner passwords:

- **Records of learner usernames and passwords for the foundation phase and Key Stage 1 learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.** *Password complexity in the foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff/teams

- **Each administrator should have an individual administrator account, as well as a user account with access levels set at an appropriate level. Consideration should also be given to using two-factor authentication for such accounts**.
- **An administrator account password for the school systems should also be kept in a secure place e.g. school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account**
- **Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.**
- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by Imraan Rawat IT Technician. Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.
- Requests for password changes should be authenticated by Imraan Rawat IT Technician to ensure that the new password can only be passed to the genuine user. Requests will be authorised by HT for a request by a member of staff or by a member of staff for a request by a learner.

Audley Infant School

School Technical Security Policy (including filtering and passwords)

- Visitors will be provided with a generic email with appropriate access to systems. Access will be logged by office staff
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on the screen and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

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

- at induction
- through the school's online safety policy
- through the acceptable use agreement

Learners will be made aware of the school's/college's password policy:

- in lessons as appropriate

Audit/Monitoring/Reporting/Review:

The responsible person Helen Nelson/Imraan Rawat IT Technician will ensure that full records are kept of:

- User Ids and requests for password changes
- User logins
- Security incidents related to this policy

Filtering - Fortinet

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or 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. The school must have a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

DfE Keeping Learners Safe in Education requires schools to have "appropriate filtering". Guidance can be found on the UK Safer Internet Centre site.

Schools may wish to test their filtering for protection against illegal materials at SWGfL Test Filtering

Responsibilities

The responsibility for the management of the school's filtering policy will be held by Helen Nelson Headteacher. They will manage the school filtering, in line with this policy and will keep records/logs of changes and 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, Imraan Rawat IT Technician:

All users have a responsibility to report immediately to Helen Nelson Headteacher, any infringements of the school's filtering policy of which they become aware or any sites that are accessed, that they believe should have been filtered.

Users must not attempt to use any programs 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 filtering provider Fortinet, 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.

- Mobile devices that access the school's 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 Helen Nelson the Headteacher and Imraan Rawat IT technician.
- In the event of the technical staff needing to switch off the filtering for any reason, or any user, this must be logged and carried out by a process that is agreed upon by the Headteacher (or other nominated senior leader).

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the online 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 online safety information contained on the website.

Changes to the Filtering System

In this section the school should provide a detailed explanation of:

- A request to make changes to the filtering system will be made to Helen Nelson Headteacher. The change is undertaken by the BwD IT department which manages the Fortinet software

- Changes will be considered to support pupils' education and improved access to learning sites
- Changes will be monitored by the Senior Leadership Team through curriculum monitoring activity

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 Helen Nelson Headteacher will decide whether to make school-level changes (as above).

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 school equipment as indicated in the school online safety policy and the acceptable use agreement. All pupil internet access will be facilitated and closely monitored by a member of the teaching staff at all times during the school day.

Audit/Reporting

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

- Health and Safety Committee/Governor with responsibility for Safeguarding
- External Filtering provider/Local Authority/Police on request

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

Further Guidance

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).

The Department for Education 'Keeping Children Safe in Education' requires schools 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"

Somerset Guidance for schools – questions for technical support – this checklist is particularly useful where a school uses external providers for its technical support/security.

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

Audley Infant School

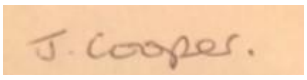
School Technical Security Policy (including filtering and passwords)

Policy agreed by

H Nelson Headteacher

Signed Date 4th September 2023

J Cooper Chair of Governors/Safeguarding Link Governor



Signed Date 4th September 2023