Hywel Dda Primary School
Technical Use Policy
September 2025

Version Control:

Version	Last Modified	Last Modified By	Document Changes	Date presented to and agreed by Governing Body
1	July 2025	James Jones	Full update	

UNCRC:

16. Protection of privacy

Every child has the right to privacy. The law must protect children's privacy, family, home, communications and reputation (or good name) from any attack.

17. Access to information

Children have the right to get information from the Internet, radio, television, newspapers, books and other sources. Adults should make sure the information they are getting is not harmful. Governments should encourage the media to share information from lots of different sources, in languages that all children can understand.

Personal Use Policy

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 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 user's files (other than that allowed for monitoring purposes within the school's policies – for example, senior staff can access pupils' Hwb accounts).
- 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 devices.
- User activity is monitored and filtered, and that adequate processes are in place to detect and respond to incidents.
- 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 Online Safety Lead plus the LA's technical team.

Technical Security

Policy statements

The school will be responsible for ensuring that their infrastructure 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 (if not managed by the Local Authority, these may be outlined in local authority/other relevant body technical/online safety policy and guidance).
- 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, end-user 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 (local authority or managed provider level).
- 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/other person and will be reviewed, at least annually, by the Online Safety 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 logon details and must immediately report any suspicion or evidence that there has been a breach of security (see password section below).
- Bethan Davies – admin 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. (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.)
- Device security and management procedures are in place (where devices are allowed access to school systems).
- School/local authority/managed service provider 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 Online Safety Lead.
- An agreed policy is in place for the provision of temporary access of "guests", onto the school technical system. (Device Management Policy and Hwb Policy for non-MIS users)
- An agreed policy is in place regarding the downloading of executable files and the installation of programs on school devices by users. (Device Management Policy)
- An agreed policy is in place regarding the extent of personal use that users (mainly staff) and their family members are allowed on school devices that may be used out of school. (Device Management Policy)
- An agreed policy is in place regarding the use of removable media (e.g. USB pen drive/CDs/DVDs) by users on school devices (Personal Data Policy)
- The school infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats such as viruses, malware, and ransomware. (Cyber security all managed by the LA)
- Personal data cannot be sent over the internet or taken off the school site unless encrypted or otherwise secured. (See Data Protection suite of policies on school website).

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 platform). Where sensitive data is in use – particularly when accessed on personal devices – schools may wish to use more secure forms of authentication e.g. two factor authentication.

Further guidance can be found from the Hwb Support Centre, 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 (learners and staff) have responsibility for the security of their username and password, must not allow other users to access the systems using their logon 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 Hwb for all staff and pupils, plus the LA for staff access to relevant networks, 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, number 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 the school.
- Staff should not use or encourage the use of the same or similar passwords for multiple users. Passwords should be unique for each user.
- 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.
- The school may wish to recommend to staff that they make use of a password manager that can store passwords in an encrypted manner and can generate very difficult to crack passwords.
- Passwords should not be set to expire if they comply with the above but should be unique to each service the user logs into.

Learner passwords:

Primary schools will need to decide at which point they will allocate individual usernames and passwords to learners. Schools should use individual logons wherever possible: in the case of Hwb these may already have been provisioned for you.

Whilst schools may choose to use class logons for services other than Hwb, these should be implemented with caution as schools need to be aware of the risks associated with not being able to identify any individual. Use by learners in this way should always be supervised and members of staff should never use a class logon for their own network/internet access. Schools should also consider the implications of using whole class logons when providing access to virtual learning environments and applications, which may be used outside school.

- Passwords for PS1 and 2: Records of learner usernames and passwords for foundation phase 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 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.
- Password requirements for learners at PS3 should increase as learners progress through school.
- Users will be required to change their password if it is compromised. Some schools may choose to reset passwords at the start of each academic year to avoid large numbers of forgotten password reset requests where there is no user-controlled reset process. (Note: passwords should not be regularly changed but should be secure and unique to each account.)

- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- Schools may wish to add to this list for all or some learners any of the relevant policy statements from the staff section above.

Notes for technical staff/teams

- Where possible, each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level.
- Consideration should also be given to using two factor authentication for administrator 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. (A school should never allow one user to have sole administrator access)
- 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 The Online Safety Lead or the Admin Manager. 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.
- Where automatically generated passwords are not possible, then a good password generator should be used by the Online Safety Lead or Admin Manager to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.
- Requests for password changes should be authenticated by Online Safety Lead or Admin Manager to ensure that the new password can only be passed to the genuine user.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expire after use. (For example, the technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)
- In good practice, the account is “locked out” following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption).

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. It is also essential that users be taught how passwords are compromised, so they understand why things should be done a certain way.

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

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

- in lessons (the school should describe how this will take place)
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review

The responsible person (the Online Safety Lead) will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- 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.

The school's connectivity and online access if provided through the LA. This provides strict filtering and cyber security.

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 the LA. 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 will be reported and logged by the LA.

All users have a responsibility to report immediately to the Online Safety Leader 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 applications 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 their Internet Service Provider and the local authority.
- The only way to overcome the filtering system is to put ina. request to the LA to request access to blocked web content
- 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
- School owned mobile devices are subject to the same filtering standards when used on external networks as they do when on the school system.
- 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 in the LA.

Education/Training/Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). 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 the newsletter.

Changes to the Filtering System

- Only staff may request changes to the filtering system
- There should be strong educational reasons for changes that are agreed
- 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 Leader who will decide whether to make school level changes (as above) and will contact the LA as needed.

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/equipment as indicated in the school Online Safety Policy and the acceptable use agreement.