YSGOL
CEFNLLYS

Cyber Security Policy

Author	M. Soporova
Responsibility	All staff and the governing body
Effective Date	October 2025
Review Date	October 2026
Approved by Governing Body	January 2026
Storage: (i) Electronic (ii) Hard Copy	(i) e.g. School network - Teams (ii) Policy file
The named ICT and on online Safety coordinators in this school are:	Michaela Soporova
Distribution & availability	All staff and governors – Electronic and hard copy available in the school office Other stakeholders – Electronic copy on the website, hard copy on request.

Policy History

Dat of the update	Summary of changes	Page number	Author

Contents

Policy Statement

Purpose

This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human error, hacker attacks and system malfunctions could cause great damage and may jeopardise our school's reputation or threaten our finances.

For this reason, a number of security measures are defined within this policy as absolute requirements. Our commitment to achieve those measures and their outcomes will be documented, reviewed, and analysed on a regular basis.

The Policy will also define Cyber security measures that may help mitigate security risks.

The Policy is based on current guidance provided by the National Cyber Security Centre (NCSC) **10 Steps to Cyber Security**

Scope

This policy applies to all our staff, governors, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Roles and Responsibilities

As managing ICT and online-safety are important aspects of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility for the Security of their systems and the data they contain and to therefore ensure that the policy and practices are embedded and monitored.

Governors

- The Governors will ensure that the school has a security policy and that this has been implemented.
- Governors will delegate the day to day implementation of the policy to the Head Teacher

- The Governors recognise and accept their corporate responsibility to provide a safe and secure environment for children, employees and visitors to the school. The school's security procedures will operate within the framework described in this policy.
- Where appropriate the Governors will seek any necessary expert advice to determine the security risks and precautions required to deal with them.
- The Governing Body will provide staff with enough resources, information and training to implement the security procedures.
- The Governing Body will, where appropriate, be informed of breaches and failures of the policy to enable them to take any corrective action as is necessary to ensure the safety of children and staff
- Governors will monitor the performance of the school security measures. This will be achieved
    - via the head teachers reports to governors
    - by all governors observing its implementation when they visit the school.
    - Governors will periodically review the school's security policy and implementation documentation.

Head Teacher

The head teacher will:

- Set up arrangements in school that comply with the security policy agreed by governors.
- Ensure that all staff within the school receive information, instruction and training in the security policy and procedures.
- Establish a system for the reporting, recording and investigation of breaches of the policy and take reasonable steps to prevent reoccurrence.
- Ensure that all visitors, contractors and agency staff adhere to the security policy.
- Monitor the implementation of the policy and security arrangements.

Staff

- All staff will comply with this policy and the arrangements made by the Head Teacher to ensure the safety of children, employees and others on the school site.
- Specific responsibilities for identified school security issues will be allocated and recorded within this policy by the Headteacher.

Children

- Children will be encouraged to exercise personal responsibility for the security of themselves and others.
- Children will cooperate with the arrangements made for the security of the school and its information systems. Breaches of the school security arrangements are a breach of the school's Behaviour Policy

Definitions

Data

Confidential data is private and valuable. Common examples are:

- Data of students/parents/carers
- Financial data
- Personal information

Example of the data and information in use

- Student and Staff information in our Management Information System (e.g. SIMS, Teacher Centre)
- Sensitive information of some pupils e.g. LAC, ALN, Child Protection
- Communication – emails and messages through e.g. Hwb
- Curriculum and Teaching materials
- Records of information (meetings, presentations, etc)

All staff are obliged to protect this data. In this policy, we will give staff instructions on how to avoid information and Cyber security breaches.

Threats and vulnerabilities

A vulnerability, coupled with an active threat, and if left untreated could cause a cyber security incident. This could disrupt the day-to-day operations of the school, the delivery of education and could cumulate in a serious incident which could result in a penalty from the information commissioner and a costly exercise to recover from.

As part of the policy implementation and guidance is it imperative, we identify vulnerabilities within the Information technology environment and implement measures to reduce the risk of these threats materializing. The following Strategy and policy implementation will define the measures in place to mitigate the most common Cyber Security risks.

Policy Implementation

Cyber Security Strategy

The School will have a 5 step strategy to Cyber Security.

- Defend
- Detect
- Protect
- Respond
- Recover

Defend

The School will implement measures to defend against the most common Cyber attacks including

- Protection within the email system against Phishing and Malware Bourne attacks.
- Accounts will be protected with strong passwords, Multi Factor Authentication will be present on any Internet facing systems.
- Network segregation from less trusted networks (e.g Internet) by a firewall.
- Utilise the Web Filtering protection made available by the Network Provider.
- Ensure there is sufficient AntiVirus/Anti Malware protection installed on all devices.
- Ensure that all software, including Operating system software is fully maintained in active support and regularly patched against vulnerabilities.
- Restrict the use of free to download software on school devices.

Detect

The school will have some basic steps in place in order to detect a potential cyber security incident.

- Anti Virus/Malware software will be in place, updated regularly and will generate alerts to potential virus incidents.
- Ensuring anomalies and events are detected, and their potential impact is understood

Protect

The school will have sufficient procedures in place to protect against unauthorised access to its systems and information.

- Identity Management and Access Control within the organisation including physical and remote access.

- Training and awareness programmes will be in place to ensure staff are fully briefed on cyber threats and conscious of their actions.
- Data Protection is considered in regards to the technical controls implemented to protect the Confidentiality, Integrity and Availability of Personal Data.
- Implement information protection processes and procedures to maintain and manage the protection of information systems and assets

Respond

The school will have in place a response plan to an anticipated Cyber Security Incident.

- There will be a Cyber Security Incident Management plan in place
- Staff should be made fully aware of how to report a cyber security incident including when and how.
- There should be procedures on which actions can be undertaken immediately to mitigate the effects of a Cyber security Incident.
- Communication plans should be well documented and circulated to all senior staff.

Recover

The School will have in place an ICT business continuity and disaster recovery plan

- The School will have a backup plan for all systems and data.
- Where Data storage is outsourced to a third party, backup and recovery procedures should be in place and part of the service delivery contract.
- Lessons learnt will be part of the recovery plan and implemented into further Business Continuity plans

10 steps to Cyber Security

Risk Management

The School has identified Cyber Threat as a risk and as such will implement sufficient controls to address the most common Cyber Security threats. The school will have a risk register containing cyber threats and their potential consequences and will detail the mitigations in place to reduce the risk to an acceptable level.

The governing body will have sight of the risk register and will be responsible for accepting the level of risk that remains.

Engagement and Training

All staff will undertake Cyber Security Training on an annual basis. Head teachers will be responsible for promoting and enforcing this within the school.

Asset Management

All physical devices will be recorded and their approximate locations known. Assets should be marked as property of the school.

All devices must be regularly updated with Security Patches, and have supported Operating systems. Unsupported and legacy software and systems which do not receive security updates should not be used.

Information (Data) assets when stored on devices, including removable media must be protected by device encryption.

Responsibilities for Asset management must be clearly defined and communicated.

Critical assets which support a core function should be protected from Cyber threats and clear responsibilities defined for the maintenance and protection of those assets.

Architecture and Configuration

A Secure Architecture to protect devices from unauthorised access will be maintained and responsibilities clearly defined for maintaining that architecture.

Direct access to the schools network infrastructure will be prevented by the installation of a firewall between the network and less trusted networks such as the Internet.

Mobile Device management software should be in place to manage portable devices, this will be capable of initiating remote wipe functions.

Vulnerability Management

Ensure all equipment used by the school is included in an active patch and upgrade process. Responsibilities for deploying patches and upgrades to all systems must be defined and clear timescales for deploying those upgrades defined. All Critical patches should be deployed with 14 days. For devices that are not automatically updated, this should detail how and when updates get applied, and who is responsible for doing and checking the updates.

Any systems which the school has responsibility for will be regularly updated.

Any known vulnerabilities which cannot be remediated will be assessed and recorded on the schools risk register, consideration to segregation from the network will be given.

For devices that are not automatically updated, this should detail how and when updates get applied, and who is responsible for doing and checking the updates.

Identity and Access Management

Access to data, systems and services need to be protected. Appropriate methods will be established to prove the identity of users, devices, or systems, with enough confidence to make access control decisions.

All system containing Personal Sensitive Confidential or business critical (financial) must be protected by sufficient authentication to prevent unauthorised access. Password policies must be enforced on all systems and where applicable Multi Factor authentication used, especially in the case of Administrative access and access to Internet based systems.

There will be a process in place to ensure access to systems and data is reviewed in when there are changes in employment.

All portable devices that are capable of storing information must be encrypted and will have appropriate authentication requirements before allowing access to the device.

If third parties require access to systems, there should the relevant Data protection and non-disclosure agreements in place and arrangements in place to revoke any accesses when necessary.

Monitoring , Reporting and alerting of unauthorised access will be implemented wherever possible.

Data Security

Data that is identified as important to the running of the school, Personal, Confidential, Business critical or has the need to be protected from authorised access will have appropriate security measures applied to enforce that protection, including access to and the sharing of this information when stored electronically. Data that is copied or stored on removable media must be encrypted.

There will be an appropriate Backup and Restore procedures which can be regularly tested. There will be Disaster recovery procedures which can be implemented stating clear responsibilities for who can initiate the procedures and who can implement it in order to recover critical data to a known safe condition.

Data should be backed up to an offsite location and be protected from unauthorised access to prevent backup corruption or complete data loss.

It must be clearly known and documented how backups are configured and who is responsible for ensuring they take place and can be regularly tested.

Information Handling

There will be procedures in place informing staff of how and where to store the schools information records and in addition how to share information securely using the system in use in the school e.g Email, Office 365 inc Sharepoint.

Disposal of redundant school ICT equipment

There will be clear procedures for the disposal of redundant ICT equipment via Powys Count Council IT services (or the name of the company/organisation that do this for the school). The school will ensure that a; data is removed from devices prior to disposal.

Logging and Monitoring

Sufficient logs should be in place to enable the school to investigate unauthorised access to systems. Audit logging will generally be implemented on the schools authentication system or with HWB. The school will document systems and ensure they are aware of whose responsibility the logging and auditing responsibility is.

Incident Management

Incident management is a key part of the Respond section of the Strategy, The school will have an indent management procedure in place

Supply chain Security

The School will understand the supply chain, including commodity suppliers such cloud service providers and those suppliers they hold a bespoke contract with. There will be a key contact details list maintained for all suppliers (third party contracts, systems support companies etc)

Whenever the school enters into a new contract with a supplier for ICT systems and services, the school will conduct Data Protection impact assessment and Supplier security audits to ensure the supplier is suitably qualified to process information and maintain systems on behalf of the school.

Cyber Security controls

Take security seriously

Everyone, from our customers and partners to our staff and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Protect personal and school devices

In general, staff should try to only use school-issued devices to access school emails, accounts or folders. When staff use personal digital devices to access school emails or accounts, they introduce a security risk to our data. We advise our staff to keep both their personal and school-issued computer, tablet and mobile phone secure. They can do this if they:

- Keep all devices password protected
- Ensure that the school-installed antivirus software is installed on their school-owned computer and that they have anti-virus software installed on home computers/devices.
- Ensure they do not leave their devices exposed or unattended.
- Ensure that school-wide security updates of browsers and systems have taken place.
- Log into school accounts and systems through secure and private networks only.

We also advise our staff to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive school-issued equipment they will receive instructions and guidance relating to the guidelines above and they must sign an ICT acceptable use agreement.

Antivirus / anti-malware software is installed on all school-owned laptops / devices and we advise all staff to have anti-virus software installed on their own devices.

Staff must follow instructions to protect their devices and refer to our IT Provider / Network manager with any queries or concerns.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct staff to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.

- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If a member of staff isn't sure that an email they received is safe, they can refer to Partnership Education.

See the section in the Acceptable Use of ICT Policy for further details on email etiquette and email security.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our staff to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays). General guidance on creating a password is to take three random words and to add a number and a special character – eg. DinosaurStarRose14%
- Remember passwords instead of writing them down. If staff need to write their passwords, please keep passwords and identifiers separate or, at least, secure.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, staff should prefer the phone instead of email, and only if they personally recognize the person they are talking to.

- Whilst some providers and organisations with whom we work advise (and expect) passwords to be changed regularly, we advise that passwords only be changed if and when they are compromised.

Transfer data securely

Transferring data introduces security risk. Staff must:

- Avoid transferring sensitive data (e.g. customer information, staff records) outside of schools systems unless absolutely necessary. When mass transfer of such data is needed, we request staff to ask our IT provider (Insert Provider name) for help.
- Share confidential data over the school network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.

- Ensure that data is sent to the correct email addresses/contacts and take particular care when sending mass emails (eg. via BCC facility)
- Report scams, privacy breaches and hacking attempts
- Our IT Provider needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we require our staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Provider will investigate promptly, resolve the issue and send a schoolwide alert when necessary.

Our IT provider and network manager is responsible for advising staff on how to detect scam emails. We encourage our staff to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct staff to:

- Turn off screens and lock devices when leaving desks.
- Report stolen or damaged equipment as soon as possible to
- Change all account passwords at once if a device is stolen.
- Report a perceived threat or possible security weakness in school systems.
- Refrain from downloading suspicious, unauthorised or illegal software on school equipment.
- Avoid accessing suspicious websites.

We also expect staff to comply with our Acceptable Use of ICT policies.

Our IT provider/ Network Administrators will:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training for all staff.
- Inform staff regularly about new scam emails or viruses and ways to combat them.
- Provide assistance to Investigate security breaches thoroughly when required.
- Follow this policy's provisions as other staff do.

Working remotely

Anyone working remotely for whatever reason, must follow this policy's instructions too. When staff are accessing our school's systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage staff to seek advice from our IT Administrators.

Reporting incidents, abuse and inappropriate materials

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the school's Data Protection Officer and Headteacher.

The school's DPO is : Michaela Soporova

Pease refer to the Schools Incident Response plan for detailed guidance on incident response.

To report cyber security incidents contact : ictservicedesk@powys.gov.uk or 01597 826100 (a phone call may be required if your whole system has been compromised and emails cannot be sent)

Additional make the IT Support provider for the school aware, servicedesk@ceredigion.gov.uk

Report personal data breaches to information.compliance@powys.gov.uk.

Where necessary you may need contact the National Cyber Security Centre (https://report.ncsc.gov.uk/), and Action Fraud (https://www.actionfraud.police.uk/)
It may be appropriate to seek advice from Powys ICT service beforehand

ICO – Data breach reporting - UK GDPR data breach reporting (DPA 2018) | ICO

Disciplinary Action (please review this section and amend in line with school policy)

We expect all our staff to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal or written warning and train the staff on security.

Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

- We will examine each incident on a case-by-case basis.
- Staff who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn’t resulted in a security breach.