E-Security Policy

Prepared/Updated : May 2023

Review Frequency : 2 Years

Next Review Due : May 2025

Contents:

Statement of intent

Penwortham Priory Academy is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The school recognises, however, that breaches in security can occur. In schools, most breaches are caused by human error, so the school will ensure all staff are aware of how to minimise this risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks, the school will ensure there are procedures in place to prevent attacks occurring.

As a result, the school has created this E-Security Policy to ensure that appropriate mechanisms of control are put in place to effectively manage risks that arise from internet use.

1. Legal framework

1.0. This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ESFA (2022) 'Academy trust handbook 2022'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- (DfE) 'Meeting digital and technology standards in schools and colleges'

1.1. The school will implement this policy in conjunction with the following policies:

- Acceptable Use Policy
- E-safety Policy

2. Types of security breach and causes

2.0. **Malicious technical attacks:** These are intentional attacks which seek to gain access to a school's system and data. Often, these attacks also attempt to use the school's system to mount further attacks on other systems, or use the system for unauthorised purposes, and can lead to reputational damage.

2.1. **Accidental attacks:** These attacks are often as a result of programme errors or viruses in the school's system. Whilst these are not deliberate, they can cause a variety of problems for schools.

2.2. **Internal attacks:** These attacks involve both deliberate and accidental actions by users and the introduction of infected devices or storage into the school's system, e.g. USB flash drives.

2.3. **Social engineering:** These attacks result from internal weaknesses which expose the school's system, e.g. poor password use.

3. Roles and responsibilities

3.0. The Facilities Manager is responsible for implementing effective strategies for the management of risks imposed by internet use, and to keep its network services, data and users secure.

3.1. The Facilities Manager is responsible for the overall monitoring and management of E-Security.

3.2. The Facilities Manager is responsible for establishing a procedure for managing and logging incidents.

3.3. The Facilities Manager is responsible for ensuring the school meets the relevant E-Security standards.

3.4. The Principal will hold regular meetings with the Facilities Manager to discuss the effectiveness of E-Security, and to review incident logs.

3.5. The Trustees will review and evaluate this E-Security Policy on a regular basis in conjunction with the Principal and Facilities Manager, taking into account any incidents and recent technological developments.

3.6. The Principal is responsible for making any necessary changes to this policy and communicating these to all members of staff.

3.7. All members of staff and pupils are responsible for adhering to the processes outlined in this policy, alongside the school's E-safety Policy and Acceptable Use Policy.

4. Secure configuration

4.0. An inventory will be kept of all ICT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. This will be stored in the school asset management system and will be audited on a termly basis to ensure it is up-to-date.

4.1. Any changes to the ICT hardware or software will be documented using the inventory, and will be authorised by the Facilities Manager before use.

4.2. All systems will be audited on a termly basis to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory.

4.3. Any software that is out-of-date or reaches 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products, such that any security issues will not be rectified by suppliers.

4.4. All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed every 90 days to prevent access to facilities which could compromise network security.

4.5. The school believes that locking down hardware, such as through strong passwords, is an effective way to prevent access to facilities by unauthorised users. This is detailed in section 6 of this policy.

4.6. All devices will be set up in a way that meets the standards described in the technical requirements.

5. Network security

5.1. The school will employ firewalls in order to prevent unauthorised access to the systems.

5.2. The school's firewall will be deployed as a:

- **Localised deployment**: the broadband service connects to a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system

5.3. As the school's firewall is managed on the premises, it is the responsibility of the Facilities Manager to effectively manage the firewall. The Facilities Manager will ensure that:

- The firewall is checked regularly for any changes and / or updates, and that these are recorded using the inventory
- Any changes and / or updates that are added to servers, including access to new services and applications, do not compromise the overall network security
- The firewall is checked regularly to ensure that a high level of security is maintained and there is effective protection from external threats
- Any compromise of security through the firewall is recorded using an incident log and is reported to the Principal. The Facilities Manager will react to security threats to find new ways of managing the firewall.

5.4. The school will be aware that the security standards may change over time with changing cyber threats.

5.5. The school will ensure that the security of every device on its network is reviewed reguarly.

5.6. The school will agree a system for recording and reviewing decisions made about network security.

5.7. Unlicenced hardware or software will never be used by the school.

5.8. All unpatched or unsupported hardware or software will be replaced. Where it is not possible to replace these devices, they will have their access to the internet removed so that scanning tools can not find weaknesses.

6. User privileges and passwords

6.0. The school understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

6.1. The Principal will clearly define what users have access to and will communicate this to the Facilities Manager, ensuring that a written record is kept.

6.2. The Facilities Manager will ensure that user accounts are set up appropriately such that users can access the facilities required, in line with the Principal's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

6.3. The Facilities Manager will ensure that websites are filtered on a weekly basis for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 7 of this policy.

6.4. All users will be required to change their passwords every 90 days and must use upper and lowercase letters, as well as numbers, to ensure that passwords are strong. Users will also be required to change their password if this becomes known to other individuals.

6.5. Pupils are responsible for remembering their passwords; however, the Facilities Manager will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary.

6.6. A multi-user account will be created for visitors to the school, such as volunteers, and access will be filtered as per the Facilities Manager's instructions. Usernames and passwords for this account will be changed on a termly basis, and will be provided as required.

6.7. User provisioning systems will be employed in order to delete inactive users or users who have left the school. The Facilities Manager will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

6.8. User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data.

6.9. The school will implement a user creation, approval and removal process which is part of the school joining and leaving protocol.

7. Monitoring usage

7.0. Monitoring user activity is important for early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

7.1. The school will inform all pupils and staff that their usage will be monitored, in accordance with the school's Acceptable Use Policy and E-safety Policy.

7.2. An alert will be sent to the Facilities Manager when monitoring usage, if the user accesses inappropriate content or a threat is detected. Alerts will also be sent for unauthorised and accidental usage.

7.3. Alerts will identify the user, the activity that prompted the alert and the information or service the user was attempting to access.

7.4. The Facilities Manager will record any alerts using an incident log and will report this to the Principal. All incidents will be responded to in accordance with section 11 of this policy, and as outlined in the E-safety Policy.

7.5. All data gathered by monitoring usage will be kept in a secure location for easy access when required. This data may be used as a method of evidence for supporting a not yet discovered breach of network security.

8. Removable media controls and home working

8.0. The school understands that pupils and staff may need to access the school network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

8.1. The Facilities Manager will encrypt all school-owned devices for personal use, such as laptops, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

8.2. Pupils and staff are not permitted to use their personal devices where the school shall provide alternatives, such as work laptops and tablets, unless instructed otherwise by the Principal.

8.3. If pupils and staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school's network security. This will be checked by the Facilities Manager.

8.4. When using laptops, tablets and other portable devices, the Principal will determine the limitations for access to the network, as described in section 6 of this policy.

8.5. Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off of the school premises.

8.6. The Facilities Manager will use encrypting to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise the network security when bringing the device back onto the premises.

8.7. All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

8.8. The Wi-Fi network at the school will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for

their personal devices, such as mobile phones or tablets, unless instructed otherwise.

8.9. A separate Wi-Fi network will be established for visitors at the school to limit their access from printers, shared storage areas and any other applications which are not necessary.

8.10. Staff and pupils will adhere to data protection legislation and the school's related policies when working remotely.

8.11. Staff and pupils are not permitted to let their family members or friends use any school equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member that is found to have shared personal date without authorisation in line with the Disciplinary Policy and Procedure. This may also result in a data breach that the school would need to record and potentially report to the ICO.

8.12. Pupils are not permitted to use school-owned devices or software for activities that do not pertain to their online education, e.g use of social media, gaming and streaming.

8.13. In the even that a staff member or pupil decides to leave the school permanently, all data in any form will be returned on or before their last day.

9. Malware prevention

9.0. The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

9.1. The Facilities Manager will ensure that all school devices have secure malware protection, including regular malware scans.

9.2. The Facilities Manager will update malware protection on a regular basis to ensure they are up-to-date and can react to changing threats.

9.3. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

9.4. Filtering of websites, as detailed in section 6 of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the Facilities Manager.

9.5. The school will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

9.6. The Facilities Manager will review the mail security technology on a regular basis to ensure it is kept up-to-date and is effective.

9.7. The school will use anti-malware software that is set to scan files and web pages as soon as they are accessed or downloaded.

10. User training and awareness

10.0. The Facilities Manager and Principal will arrange training for pupils and staff on a regular basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and E-safety Policy.

10.1. Training will also be conducted around any attacks that occur and any recent updates in technology or the network.

10.2. All staff will receive training as part of their induction programme, as well as any new pupils that join the school.

10.3. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the E-safety Policy.

11. Incidents

11.0. In the event of an internal attack or any incident which has been reported to the Facilities Manager, this will be recorded using an incident log and by identifying the user and the website or service they were trying to access.

11.1. All incidents will be reported to the Principal, who will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.

11.2. In the event of any external or internal attack, the Facilities Manager will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites, etc.

11.3. If necessary, the management of E-Security at the school will be reviewed to ensure effectiveness and minimise any further incidents.

12. Monitoring and review

12.0. This policy will be reviewed every 2 years by the Facilities Manager and Principal, who will then communicate any changes to all members of staff and pupils.