Priory Woods School

E-Security Policy

Contents:

1. Legal framework
2. Types of attacks
3. Roles and responsibilities
4. Secure configuration
5. Network security
6. Managing user privileges
7. Monitoring usage
8. Removable media controls and home working
9. Malware prevention
10. User training and awareness
11. Incidents
12. Monitoring and review

Appendices

a) Additional e-security measures

Introduction

Priory Woods School staff and governors understand that use of the internet is important for day-to-day activities and for enhancing the learning of our pupils.

Whilst the internet introduces new, innovative ways to support teaching, it also brings risks, which, if not properly managed, increase the chance of harm to pupils and staff. Improperly managed internet use may lead to the loss of sensitive, confidential personal data and an inability to deliver scheduled teaching as a result of a security breach.

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 usage.

1. Legal framework

1.1. This policy has due regard to official legislation including, but not limited to, the following:

- The Human Rights Act 1998
- The Data Protection Act 1998 and 2018
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

1.2. This policy also has due regard to official guidance including, but not limited to, the following:

- The Education Network 'Managing and maintaining e-security/cyber-security in schools' 2014

1.3. The school will implement this policy in conjunction with our:

- Acceptable Use Policy.
- E-safety Policy.
- Data Protection Policy

2. Threats to security from attacks

2.1. **Malicious technical attacks:** These are intentional, and attempt to gain access to a school's system and data. Often, they also attempt to use the school's system to mount further attacks on other systems, or use the system for unauthorised purposes, which could damage the reputation of the school.

2.2. **Unintended attacks:** This may be as a result of programme errors or viruses in the school's system. Whilst they are not deliberate, they can cause a variety of problems for schools.

2.3. **Internal attacks:** These 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.

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

3. Roles and responsibilities

3.1. The Head Teacher 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.

3.2. The Network Manager is responsible for the overall monitoring and management of e-security.

3.3. The Network Manager is responsible for establishing a procedure for managing and logging incidents.

3.4. The School Business Manager and Network Manager will meet regularly to discuss the effectiveness of e-security, and to review incident logs. A summary will be presented to the Governing Body on a termly basis.

3.5. The governing body will review and evaluate this E-security Policy on a termly basis where appropriate in accordance with the School Business Manager and Network Manager taking into account any incidents and recent technological developments.

3.6. The School Business Policy 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

4.1. An inventory will be kept of all IT 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 office / ICT Office and will be audited on a termly basis to ensure it is up-to-date.

4.2. Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the Network Manager before use.

4.3. 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.

4.4. 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.

4.5. All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.

4.6. 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.

5. Network security

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

The school's firewall will be deployed as a centralised deployment: the broadband service connects to a firewall that is located within a data centre or other major network location.

5.2. As the school's firewall is managed locally, the firewall management interface will be thoroughly investigated by the Network Manager to ensure that:

- Patches and fixes are applied quickly to ensure that the network security is not compromised.
- 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 Head Teacher. The Network Manager will react to security threats to find new ways of managing the firewall.

6. Managing user privileges

6.1. 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.

6.2. The Head Teacher / School Business Manager will clearly define what users have access to and will communicate this to the Network Manager, ensuring that a written record is kept.

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

6.4. Appropriate filtering and monitoring of Internet access is in place through Smoothwall, in order to fulfill our duty of care and safeguard students and staff against any online threats and harmful content. The blocklists are automatically updated as and when new threats arise and are also checked regularly by the network manager. 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.

6.5. Users are responsible for keeping their password safe and secure; they will be required to change their password if this becomes known to other individuals.

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

6.7. Pupils will not have individual logins where appropriate and class logins will be used instead. If it is appropriate for a pupil to have their individual login, the Network Manager will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

6.8. The 'master user' password used by the Network manager will be made available to the Head Teacher and School Business Manager, and will be kept in a secure place.

6.9. A multi-user account will be created for visitors to the school, such as volunteers, and access will be filtered as per the Head Teacher's instructions. Username and password for this account will be changed on a termly basis, and will be provided as required.

6.10. The Network Manager will receive lists of users that have left the school on a weekly basis and manage the inactive users to ensure that all users that should be deleted are, and that they do not have access to the system.

7. Monitoring usage

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

7.2. 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

7.3. User access is monitored through both Securus and Smoothwall, both of which are monitored on a daily basis for alerts. Any immediate threats / issues are logged and a weekly report is created.

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

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

7.6. All data gathered by monitoring usage will be kept in a secure location, (Head Teacher's Office) 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

8.1. 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.

8.2. The Network Manager will encrypt all school-owned devices for personal use, such as laptops, USB sticks, 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.

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

8.4. 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 Network Manager.

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

8.6. 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.

8.7. The Network Manager will 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.

8.8. 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.

8.9. 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.

9. Malware prevention

9.1. 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.

9.2. The Network manager will ensure that all school devices have secure malware protection, including regular malware scans.

9.3. The Network manager will update malware protection on a termly basis to ensure they are up-to-date and can react to changing threats.

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

9.5. 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 Network manager.

9.6. 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.

9.7. The Network Manager will review the mail security technology on a termly basis to ensure it is kept up-to-date and is effective.

10. User training and awareness

10.1. The Network Manager and ICT teacher will arrange training for pupils and staff on a termly basis for pupils and on an annual basis for staff to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and E safety Policy

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

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

10.4. 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

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

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

11.3. In the event of any external or internal attack, the Network Manager will record this using an incident log and will ensure the attack does not compromise any other schools' network security.

11.4. The Network Manager will provide an appropriate response to the attack, including any in-house changes.

11.5. 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

12.1. This policy will be reviewed on a yearly basis by the governing body in conjunction with the Network Manager the School Business Manager and Head Teacher, who will then communicate any changes to all members of staff and pupils.

Additional e-security measures

In addition to firewalls, there are a number of further measures which can be employed by schools to provide a greater network protection. An example of these can be seen in the table below.

Protection	What is it?
Intrusion detection system (IDS)	An IDS is a network security technology which is able to detect malicious content by monitoring systems.
Intrusion prevention system (IPS)	An IPS is additional to an IDS, and is able to block malicious content as well as detect them.
Heuristic Threat Analysis (HTA)	HTA can detect different variants of viruses (modified forms), as well as new and previously unknown malicious content.
Penetration testing	Penetration testing is an organised attack on a system, which identifies security vulnerabilities and weaknesses in order for suitable patches to be applied.