E-Security Policy

Policy Reviewed: Autumn 2018

Agreed by Governors:

Next Review:

Headteacher's Signature:

M Robson

Chair of Governor's Signature:

C James

Contents:

Statement of intent

At Holley Park Academy we understand that use of the internet and broadband 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 a number of risks, which, if not properly managed, drastically 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 academy 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

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
- 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

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

1.1. The academy will implement this policy in conjunction with our:

- Acceptable Use Policy.
- Online Safety Policy.

2. Types of attack

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.

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.

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.

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

3 Roles and responsibilities

The headteacher 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.

The ICT technician is responsible for the overall monitoring and management of e-security.

The headteacher is responsible for establishing a procedure for managing and logging incidents.

The governing body will hold regular meetings with the headteacher to discuss the effectiveness of e-security, and to review incident logs.

The governing body will review and evaluate this E-security Policy on an annual basis in accordance with the headteacher and ICT technician, taking into account any incidents and recent technological developments.

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

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

3. Secure configuration

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

Any changes to the IT hardware or software will be documented using the inventory and will be authorised by the ICT technician before use.

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.

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.

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.

The academy 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. Network security

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

The academy's firewall will be deployed both as:

- **Centralised deployment**: the broadband service connects to a firewall that is located within a data centre or other major network location.
- **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.

As the academy's firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the ICT technician, to ensure that:

- Any changes and updates that are logged by authorised users within the academy are undertaken efficiently by the provider to maintain operational effectiveness.
- Patches and fixes are applied quickly to ensure that the network security is not compromised.

Also, as the academy's firewall is managed on the premises, it is the responsibility of the ICT technician to effectively manage the firewall. The ICT technician 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 headteacher. The ICT technician will react to security threats to find new ways of managing the firewall.

The academy will consider installing additional firewalls on the servers in addition to the third-party service as a means of extra network protection. This decision will be made by the headteacher, taking into account the level of security currently provided and any incidents that have occurred.

5. Managing user privileges

The academy 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.

The headteacher will clearly define what users have access to and will communicate this to the ICT technician, ensuring that a written record is kept.

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

The ICT technician 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.

The 'master user' password used by the ICT technician will be made available to the headteacher, or any other nominated senior leader, and will be kept in a secure place.

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

Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the academy. The ICT technician 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. Monitoring usage

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

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

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

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

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

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.

7. Removable media controls and home working

The academy understands that 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.

The ICT technician 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.

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

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

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.

The ICT technician 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.

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.

The Wi-Fi network at the [school/academy] 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. Malware prevention

The academy 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.

The ICT technician will ensure that all school devices have secure malware protection, including regular malware scans.

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

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

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 ICT technician.

The academy 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.

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

9. User training and awareness

The ICT technician and headteacher will arrange training for pupils and staff on an annually basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and Online safety Policy.

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

All staff will receive training as part of their induction programme, if necessary.

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 Online Safety Policy.

10. Incidents

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

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

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

In the event of any external or internal attack, the ICT technician will record this using an incident log and will contact the third-party provider to ensure the attack does not compromise any other schools' network security.

The ICT technician will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.

If necessary, the management of e-security at the academy will be reviewed to ensure effectiveness and minimise any further incidents.

11. Monitoring and review

This policy will be reviewed on an annually basis by the governing body in conjunction with the ICT technician and headteacher, 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.