OWLS Academy Trust

E-Security Policy

Date Detail June 25th, 2018

Original, based on Trust Policy 25.06.17

Reviewed annually

Approved by Jonathan Tedds, Chair of Governors

Adopted by The OWLS Academy Trust on	June 25th 2018
Next Review Due	annually

At the OWLS Academy Trust 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 schools within the Trust have 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

Legal Framework

This policy has due regard to official legislation including but not limited to:

- The Human Rights Act 1998;
- The Data Protection Act 1998;
- The Regulation of Investigatory Powers Act 2000;
- The Safeguarding of 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 Education Network "Managing and Maintaining e-security/cyber-security in schools" 2014

This policy will be implemented in conjunction with:

- Acceptable Use Policy;
- E-safety Policy

Types of Attack

Malicious Technical Attacks: 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: Attacks resulting from internal weaknesses which expose the school's system, e.g. poor password use.

Roles and Responsibilities

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;
- Establishing a procedure for managing and logging incidents;
- Making any necessary changes to this policy and communicating these to all members of staff.

Local Governing Bodies will:

- Hold regular meetings with the head teacher to discuss the effectiveness of e-security, and to review incident logs;
- Review and evaluate this E-security Policy on a termly basis in accordance with the head teacher and IT technician, taking into account any incidents and recent technological developments.

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

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

Secure Configuration

An inventory will be kept of all IT hardware and software currently in use at the schools, including mobile phones and other personal devices provided by the school. This will be stored in the school office or appropriate rooms and will be audited on a regular 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 IT technician before use.

All systems will be audited on a regular 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 schools within the trust believe 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 the section of this policy headed "Managing User Privileges".

Network Security

Schools

All of the schools within the Trust will employ firewalls in order to prevent unauthorized access to the systems. These will be deployed as a "localized deployment" whereby 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 school's firewalls are managed on the premises, it is the responsibility of the IT technicians to effectively manage the firewall. The IT technicians will ensure that for their school(s):

- 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 head teacher. The IT technician will react to security threats to find new ways of managing the firewall.

Trust

For cross-trust functions a centralized deployment will apply. As this firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the IT technician to ensure that:

- Any changes and updates that are logged by authorised users within the school and or 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.

The trust 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 CEO and head teachers, taking into account the level of security currently provided and any incidents that have occurred.

Managing User Privileges

The schools and the Trust understand 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 from members of staff. The head teacher will clearly define what users have access to and will communicate this to the IT technician, ensuring that a written record is kept.

The IT technician 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.

The IT 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 the next section of this policy (Monitoring Usage).

All users will be required to change their passwords on a regular basis 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.

Pupils are responsible for remembering their passwords. However, the IT technician will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary. Pupils in key stage 1 will not have individual logins and class logins will be used instead. If it is appropriate for a pupil to have their individual login, the IT technician will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

The “master user” password used by the IT technician will be made available to the head teacher, or any other nominated senior leader, and will be kept in a secure place, e.g. strong room or office areas.

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. Usernames and passwords for this account will be changed on a regular 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 school/Trust. The IT 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.

Monitoring Usage

Monitoring user activity is important for early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. All pupils and staff will be informed, by their school, that their usage will be monitored, in accordance with the Acceptable Use Policy and E-safety Policy.

An alert will be sent to the IT 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 IT technician 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 the “Incidents” section of this policy, and as outlined in the E-safety Policy.

All data gathered by monitoring usage will be kept in a secure location, offices or strong room, 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.

Removable Media Controls and Home Working

The schools understand that pupils and staff may need to access their 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 IT 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 schools shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the head teacher.

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 IT technician.

When using laptops, tablets and other portable devices, the head teacher will determine the limitations for access to the network, as described in the section of this policy relating to user privileges.

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 IT 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 schools 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.

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

Malware Prevention

The schools understand 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, and 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 school's hardware and software.

Filtering of websites, as detailed elsewhere in this policy, will ensure that access to websites with known malware is blocked immediately and reported to the IT technician.

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

User Training and Awareness

The IT technician and head teacher 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. 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, and any new pupils joining the schools will also receive appropriate instruction.

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.

Incidents

In the event of an internal attack or any incident which has been reported to the IT 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 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.

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

Localised Deployments (Schools)

In the event of any external or internal attack, the IT 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.

Centralised Deployments (Trust)

In the event of any external or internal attack, the IT 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 IT technician will work with the third party provider to provide an appropriate response to the attack, including any in-house changes.

Monitoring and Review

This policy will be reviewed on an annual basis by the Academy Trust in conjunction with the IT technicians and head teachers, 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. Examples include:

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