Collective
Vision Trust

E-Security Policy

Contents:

Statement of intent

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, Collective Vision Trust 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.

This policy applies to all schools that are part of the Collective Vision Trust.

Signed by:

Lynn Jackson	CEO	Date:	October 2019
Sarah Gribbin	Chair of Board	Date:	October 2020

1. Legal framework

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

- The Human Rights Act 1998
- The General Data Protection Regulation
- 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

2. Types of attack

2.1. **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.

2.2. **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.

2.3. **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.

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

3. Roles and responsibilities

3.1. 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.

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

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

3.4. The headteacher will regularly report to the governing body on the effectiveness of e-security, and to review incident logs.

3.5. The governing board will review and evaluate this E-security Policy on an annual basis in accordance with the headteacher and Technical Manager taking into account any incidents and recent technological developments.

3.6. The data protection officer (DPO) 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.

4. Secure configuration

4.1. An inventory will be kept of all IT hardware currently in use at the school. This will be stored in the asset database 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 asset database, and will be authorised by the IT Technicians before use.

4.3. All systems will be audited regularly 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. All hardware, software and operating systems will require passwords for individual users before use with the exception of a few pre-approved whitelisted educational websites on the shared iPads.

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.

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 ICT Technicians 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 reported to the headteacher, who will ensure that it is recorded. The Technical 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 headteacher will decide what users have access to and will communicate this to the Technical manager.

6.3. The ICT Technicians 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.

6.4. The ICT Technicians 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 reportd to the headteacher or DSL.

6.5. Users will also be required to change their password if this becomes known to other individuals.

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

6.7. The Technical manager will be informed when any user leaves the school. The Technical Manager will 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. An alert will be sent to the ICT Technicians 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. All data gathered by monitoring usage will be kept in a secure location electronic 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

8.1. 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 ICT Technicians will encrypt all school-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets. 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 provides alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the headteacher.

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. Any device which is configured for use with school email will be password or passcode protected.

8.5. Data, wherever possible, 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. 'One Drive' will be rolled out to all users as soon as possible.

8.6. The Wi-Fi network at the school will be password protected and will only be given out as required.

8.7. 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.

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

9.3. 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.

9.4. 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.

10. Incidents

10.1. 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.

10.2. All incidents will be reported to the headteacher, who will issue disciplinary sanctions to the pupil or member of staff,

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

10.4. The headteacher will report any incident that compromises the rights and freedoms of individuals to the ICO within 72 hours.

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

11. Monitoring and review

11.1. This policy will be reviewed on an annual basis by the governing board in conjunction with the headteacher, ICT technician and DPO, 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.