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 21
Sarah Gribbin	Chair of Board	Date:	October 21

Review Date: October 22

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
- National Cyber Security Centre (2018) 'Cyber Security: Small Business Guide'

1.2. This policy also has due regard to all school and trust policies and 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 security breach and causes

2.1. **Unauthorised use without damage to data** – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

2.2. **Unauthorised removal of data** – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

2.3. **Damage to physical systems** – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

2.4. **Unauthorised damage to data** – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

2.5. Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.

- Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

2.6. Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten

3. Roles and responsibilities

3.1. The data protection officer (DPO) is responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use, and for keeping the school's network services, data and users safe, in conjunction with the Technical Manager
- Leading on the school's response to incidents of data security breaches.
- Assessing the risks to the school in the event of a data security breach.
- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the Technical Manager and Headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security and preventing breaches.
- Monitoring the effectiveness of this policy, alongside the Technical Manager and Headteacher, and communicating any changes to staff members.

3.2. The Technical Manager is responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the schools in the Trust.

- Ensuring any software that is out-of-date is removed from the school premises.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Ensuring all school-owned devices have secure malware protection and that devices are regularly updated.
- Installing, monitoring and reviewing filtering systems for the school's network.
- Setting up user privileges in line with recommendations from the headteacher.
- Maintaining an up-to-date inventory of all usernames and passwords.
- Removing any inactive users from the school's system, ensuring that this is always up-to-date.
- Recording any alerts for access to inappropriate content and notifying the headteacher.
- Installing appropriate security software on staff members' personal devices where the headteacher has permitted for them to be used for work purposes.
- Performing a back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Organising training for staff members on network security.

3.3. The headteacher is responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Defining users' access rights for both staff and pupils, communicating these to the Technical Manager and maintaining a written record of privileges.
- Responding to alerts for access to inappropriate content.
- Informing the Technical Manager of staff members who are permitted to use their personal devices for work purposes so that appropriate security methods can be applied.
- Issuing disciplinary sanctions to pupils or members of staff who cause a data security breach.
- Organising training for staff members in conjunction with the Technical Manager and DPO.

4. Secure configuration

4.1. An inventory will be kept of all ICT hardware and software 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 ICT hardware or software will be documented using the asset database, and will be authorised by the ICT 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. Any software that is out-of-date or reaches its '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.

4.5. 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.

4.6. 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.

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 and DPO, who will ensure that it is recorded. The

Technical Manager will react to security threats to find new ways of managing the firewall.

6. Malware prevention

6.1. 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.

6.2. The Technical Manager and ICT Technicians will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements.

6.3. The Technical Manager and ICT Technicians will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats.

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

6.5. Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the Technical Manager.

6.6. 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.

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

6.8. Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the Technical Manager

6.9. Where apps are installed, the Technical Manager and ICT technicians will keep up-to-date with any updates, ensuring staff are informed of when updates are ready, how to install them, and that they should do this without delay.

7. Managing user privileges

7.1. 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.

7.2. The headteacher will decide what users have access to and will communicate this to the Technical manager.

7.3. 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.

7.4. 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 reported to the headteacher or DSL.

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

7.6. 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.

7.7. 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.

7.8. The master user account accessed by the Technical Manager, DPO and headteacher is subject to a two-factor authentication for logins. This account requires two different methods to provide identity before logging in – these are:

- A password; and a
- Code sent to another school-owned device, such as a tablet, which must be entered following the password.

7.9. The master user account is used as the 'administrator' which allows designated users to make changes that will affect other users' accounts in the school, such as changing security settings, monitoring use, and installing software and hardware.

7.10. 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.

7.11. The Technical Manager will review the system on a regular basis to ensure the system is working at the required level.

8. Monitoring usage

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

8.2. 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.

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

8.4. 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.

9. Removable media controls and home working

9.1. 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.

9.2. 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.

9.3. 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.

9.4. 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.

9.5. 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.

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

9.7. 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.

10. Backing-up data

10.1. The ICT Technicians perform a back-up of all electronic data held by the school on a daily or weekly basis depending on data being backed up via disk to disk as a hot backup. The date of the back-up is recorded using a log. Each back-up is retained for three months before being deleted.

10.2. The ICT technicians performs a disk to tape back-up on a weekly basis of the data stored on the backup server as a cold backup.

10.3. Where possible, back-ups are run overnight and are completed before the beginning of the next school day.

10.4. Upon completion of back-ups, data is stored on the school's hardware which is password protected. Tape backups are stored in a locked fireproof safe.

10.5. Only authorised personnel are able to access the school's data.

11. Avoiding phishing attacks

11.1. The ICT technicians will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs.

11.2. Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account.

11.3. Two-factor authentication is used on any important accounts, such as the master user account.

11.4. In accordance with section 12 of this policy, the Technical Manager and Headteacher will organise regular training for staff members – this will cover identifying irregular emails in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual.

11.5. Staff will use the following warning signs when considering whether an email may be unusual:

- Is the email from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is the email addressed to a 'valued customer', 'friend' or 'colleague'?
- Does the email contain a veiled threat that asks the staff member to act urgently?
- Is the email from a senior member of the school asking for a payment?
- Does the email sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.

11.6. The Technical Manager will ensure that email filtering systems, applied in accordance with section 6 of this policy, are neither too strict or lenient; filtering that is too strict may lead to legitimate emails becoming lost, and too lenient filters may mean that emails that are spam or junk are not sent to the relevant folder.

11.7. To prevent hackers having access to unnecessary public information, the DPO and Headteacher will ensure the school's social media accounts and websites

are reviewed on a regular basis, making sure that only necessary information is shared.

11.8. The headteacher and DPO will ensure the school's Whole-School Social Media Accounts Practice includes expectations for sharing of information – and determines what is and is not necessary to share.

11.9. The headteacher will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about the school and themselves.

12. User training and awareness

12.1. The Technical Manager and headteacher will arrange training for pupils and staff on a regular basis to ensure they are aware of how to use the network appropriately.

12.2. The DPO will also ensure that pupils and staff have regular training on maintaining data security, preventing data breaches, and how to respond in the event of a data breach.

12.3. Training for all staff members will be arranged by the Technical Manager and DPO within two weeks following an attack, breach or significant update.

12.4. Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

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

12.6. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks.

13. Security breach incidents

13.1. Any individual that discovers a security data breach will report this immediately to the headteacher and the DPO. Either the DPO or the headteacher will inform the Technical Manager.

13.2. When an incident is raised, the DPO will record the following information:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. school-owned laptop
- Location of the equipment involved

- Contact details for the individual who discovered the incident

13.3. The school's DPO will take the lead in ensuring an investigating into the breach occurs and will be allocated the appropriate time and resources to conduct this.

13.4. The DPO, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or has been compromised.

13.5. The DPO will oversee a full investigation and produce a comprehensive report.

13.6. The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

13.7. If the DPO determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.
- The headteacher will issue disciplinary sanctions to the pupil or member of staff.
- In the event of any external or internal breach, the Technical Manager will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information.

13.8. Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.

13.9. Where the security risk is high, the DPO will establish which steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.
- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location.
- Reviewing basic security, including:
  - Changing passwords and login details on electronic equipment.
  - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

13.10. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will ensure that the police are informed of the security breach.

13.11. Where the school has been subject to online fraud, scams or extortion the DPO will also ensure it is reported this using the Action Fraud website.

13.12. The Technical Manager will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

14. Assessment of risks

14.1. The following questions will be considered by the DPO to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the DPO's report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the GDPR; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following:
  - Physical safety
  - Emotional wellbeing
  - Reputation
  - Finances
  - Identity

- Private affairs becoming public

- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?

- Who could help or advise the school on the breach? Could the Trust, external partners, authorities, or others provide effective support?

14.2. In the event that the DPO, or other persons involved in assessing the risks to the school, are not confident in the risk assessment, they will seek advice from the ICO.

15. Consideration of further notification

15.1. The DPO will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security (see 15.8 onwards for specific GDPR requirements about personal data).

15.2. The DPO will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

15.3. If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

15.4. The DPO will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.

- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.

- A way in which they can contact the school for further information or to ask questions about what has occurred.

15.5. The ICO will be consulted for guidance on when and how to notify them about breaches.

15.6. The DPO will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

15.7. The DPO will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

15.8. Where a breach is likely to result in a significant risk to the rights and freedoms of individuals, the DPO will notify those concerned directly of the breach.

15.9. Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible:
  - The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
  - The type(s) and approximate number of personal data records concerned.
- The name and contact details of the DPO or other person(s) responsible for handling the school's information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

16. Evaluation and response

16.1. The DPO will establish the root of the breach, and where any present or future risks lie.

16.2. The DPO will consider the data and contexts involved.

16.3. The DPO and headteacher will identify any weak points in existing security measures and procedures.

16.4. The DPO will work with the e-safety officer to improve security procedures wherever required.

16.5. The DPO and headteacher will identify any weak points in levels of security awareness and training.

16.6. The DPO will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

17. Monitoring and review

17.1. This policy will be reviewed on an annual basis by the Trust Board in conjunction with the CEO, Technical Manager and individual Headteachers 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.