

Cyber Security Policy

Aspire Federation

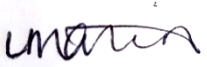


'Let your light shine!'

Reviewed and updated: November 2025

Ratified by Governors: 18th March 2026

Next review: November 2027

Signed: ... 

Name: Laura Martin
(Executive Headteacher)

Date: ...19.3.26.....

Signed: 

Name: Peter Hilton
(Chair of Governors)

Date:19.3.26.....

Contents:

Statement of intent

1. [Legal framework](#)
2. [Types of security breach and causes](#)
3. [Roles and responsibilities](#)
4. [Secure configuration](#)
5. [Network security](#)
6. [Malware prevention](#)
7. [User privileges and passwords](#)
8. [Monitoring usage](#)
9. [Removable media controls](#)
10. [Home working and remote learning](#)
11. [Backing up data](#)
12. [Avoiding phishing attacks](#)
13. [User training and awareness](#)
14. [Cyber-security breach incidents](#)
15. [Assessment of risks](#)
16. [Consideration of further notification](#)
17. [Evaluation](#)
18. [Monitoring and review](#)

Statement of intent

Aspire Federation Schools are committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The school recognises, however, that breaches in security can occur, with most breaches caused by human error. The school will ensure all staff are aware of how to minimise this risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks, the school will ensure there are procedures in place to prevent attacks occurring. To minimise both risks, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

1.1 Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO 'Guide to the General Data Protection Regulation (GDPR)'
- DfE 'Meeting digital and technology standards in schools and colleges'

This policy operates in conjunction with the following school policies:

- Online Safety Policy
- Data Protection Policy
- Disciplinary Policy and Procedure
- Behaviour Policy
- Remote Education Policy
- Code of Conduct

1.2 Types of security breach and causes

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. This includes unauthorised people within the school, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

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.

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.

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.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

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

Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision.

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the school software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g. unrestricted access to the school network, can allow unauthorised individuals to access the school system
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten

1.3 Roles and responsibilities

The governing board will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place, including any cyber response and recovery plans.
- Ensuring the school has an appropriate approach to managing data breaches in place.
- Supporting the Executive headteacher and other relevant staff in the delivery of this policy.
- Ensuring the school meets the relevant cyber-security standards.
- Ensuring at least one member of the board completes basic cyber-security training.

The Executive headteacher will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Organising training for staff members in conjunction with the online safety officer and DPO.
- Appointing an appropriately qualified staff member log of cyber-security incidents is maintained.
- Appointing a cyber recovery team who is responsible for implementing the school's procedures in the event of a cyber-security incident.

The DPO (Joe Lee, Ark) will be responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Leading on the school's response to incidents of data security breaches, including leading the cyber recovery team.
- Ensuring the plans and actions of the school relating to data and cyber security are compliant with data protection laws.
- Assessing the risks to the school in the event of a cyber-security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the ICT technicians and Executive headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security, network security and preventing breaches.
- Monitoring and reviewing the effectiveness of this policy, alongside the Executive headteacher, and communicating any changes to staff members.

The ICT technicians (currently Ark ICT) will be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- Ensuring any out-of-date software is removed from the school systems.
- Ensuring all software is kept up-to-date including running security updates/ patches.

- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Installing, monitoring and reviewing filtering systems for the school network.
- Setting up user privileges in line with recommendations from the Executive headteacher.
- Maintaining an up-to-date and secure inventory of all usernames and passwords.
- Removing any inactive users from the school system and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the Executive headteacher has permitted for them to be used for work purposes.
- Performing a secure back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Ensuring state-of-the-art encryption standards are used for all data protected by encryption.
- Ensuring all school-owned devices have secure malware protection and are regularly updated.
- Recommending and installing software to record any alerts for access to inappropriate content which will notify the Executive headteacher and other designated adults within the schools.

The online safety officer (Executive Headteacher) will be responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within the school and promoting online safety measures to parents.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy.
- Monitoring online safety incidents which could result in data breaches and reporting these to the DPO.
- Acting as the named point of contact within the school on all online safety issues.
- Liaising with relevant members of staff on online safety matters, e.g. the DPO, ICT technician, School Business Manager and Head of School.

The DSL will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security or other data breach incident and considering whether any referrals need to be made.

All staff members will be responsible for:

- Understanding their responsibilities in regard to this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

1.4 Secure configuration

An inventory will be kept of all ICT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. The inventory 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 ICT 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 by the ICT technician 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 in the inventory. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, e.g. when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords from individual users. Passwords will be changed at least annually to prevent access to facilities which could compromise network security. Passwords will need to adhere to a specific character length, use special characters, not be obvious or easy to guess, and must not be the same password used on other devices or systems, in line with the school's policy on passwords.

The school will refer to the five security controls outlined in the National Cyber Security Centre's (NCSC's) ['Cyber Essentials'](#). These are:

- **Firewalls** – Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure configuration** – The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The school will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach.
- **Access control** – The more people have access to data, the greater the risk of a security breach. The school will ensure that access is given on a 'need-to-know' basis to help protect data. All accounts will be protected with strong passwords, and where necessary, multi-factor authentication.
- **Malware protection** – The school will protect itself from malware by installing antivirus and anti-malware software – to be installed by the ICT technician.

- **Patch management** – The school will install software updates as soon as they are available to minimise the time frame in which vulnerabilities can be exploited. If the manufacturer stops offering support for the software, the school will replace it with a more up-to-date alternative.

The ICT technician will:

- Protect all devices on every network with a correctly configured boundary, or software firewall, or a device that performs the same function.
- Change the default administrator password, or disable remote access on each firewall.
- Protect access to the firewall's administrative interface with multi-factor authentication or a small, specified IP-allow list combined with a managed password, or prevent access from the internet entirely.
- Keep firewall firmware up to date.
- Check monitoring logs to help detect suspicious activity.
- Block inbound unauthenticated connections by default.
- Document reasons why particular inbound traffic has been permitted through the firewall.
- Review reasons why particular inbound traffic has been permitted through the firewall often, change the rules when access is no longer needed.
- Enable a software firewall for devices used on untrusted networks, like public wi-fi.

1.5 Network security

In line with the UK GDPR, the school will appropriately test, assess, and evaluate any security measures put in place on a **termly** basis to ensure these measures remain effective.

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

Centralised firewall deployment

The school's firewall will be deployed centrally, which means the broadband service connects to a firewall that is located within a data centre or other major network location.

As the school'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 school 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 school 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 DPO, taking into account the level of security currently provided and any incidents that have occurred.

The school will be aware that security standards may change over time with changing cyber threats, and that the security of every device on its network is reviewed regularly.

The school will agree with the ICT technician a system for recording and reviewing decisions made about network security features.

To ensure that the network is as secure as possible, the school will:

- Keep a register, list, or diagram of all the network devices.
- Avoid leaving network devices in unlocked or unattended locations.
- Remove or disable unused user accounts, including guest and unused administrator accounts.
- Change default device passwords.
- Require authentication for users to access sensitive school data or network data.
- Remove or disable all unnecessary software according to your organisational need.
- Disable any auto-run features that allow file execution.
- Set up filtering and monitoring services to work with the network's security features enabled.
- Immediately change passwords which have been compromised or suspected of compromise.
- Protect against a brute-force attack on all passwords by allowing no more than 10 guesses in five minutes, or locking devices after no more than 10 unsuccessful attempts.

Unlicensed hardware or software will never be used by the school.

All unpatched or unsupported hardware or software will be replaced by the ICT technician. Where it is not possible to replace these devices, they will have their access to the internet removed so that scanning tools cannot find weaknesses.

1.6 Malware prevention

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.

The ICT technician will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. The ICT technician will update malware protection on a **termly** basis to ensure it is 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.

Staff will follow procedures for filtering and monitoring to keep pupils safe as set out in the Online Safety Policy.

The school's filtering provider will be:

- A member of [Internet Watch Foundation](#) (IWF)
- Signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Effective at blocking access to illegal content

The filtering system will be able to identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them, and provide alerts when any web content has been blocked

Filtering of websites will ensure that access to websites with known malware are blocked immediately and reported to the ICT technician.

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

The ICT technician will download apps on any school-owned device from manufacturer-approved stores and with prior approval from the Executive Headteacher or School Business Manager. Where apps are installed, the ICT technician will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

The school will use anti-malware software that:

- Is set up to scan files upon access, when downloaded, opened, or accessed from a network folder.
- Scans web pages as they are accessed.
- Prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement.

1.7 User privileges and passwords

The school understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. pupils will have different access to data and the network than members of staff, whose access will also be role-based.

The Executive 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 to allow users access to the facilities required, in line with the

Executive headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All users will be required to change their passwords at least every two years and/or if they become known to other individuals, in line with the 'Secure configuration' section of this policy. Pupils are responsible for remembering their passwords; however, the ICT technician will have an up-to-date record of all usernames and passwords and will be able to reset them if necessary. The record of all usernames and passwords is encrypted. Only the ICT technician will have access to this inventory. Multi-factor authentication (multiple different methods of verifying the user's identity) will be used wherever possible.

The 'master user' password used by the ICT technician only.

The master user account accessed by the ICT technician will be subject to multi-factor authentication. This account will require both a password and a verification code sent to another school-owned device which must be entered following the password. 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 usage, and installing software and hardware.

A multi-user account will be created for visitors to the school, such as supply teachers, and access will be filtered as per the Executive headteacher's instructions. Usernames and passwords for this account will be provided as required.

The ICT technician will manage the system to ensure that all users that should be deleted are, and that they do not have access to the system, following written communication from the school.

Password strength will be enforced at a system level – the school will use a deny list for automatic blocking of common passwords, and passwords must contain a minimum of eight characters.

The school will implement a user account creation, approval and removal process which is part of the school joining and leaving protocols.

User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data. Users will have a separate account for routine business if their main account:

- Is an administrative account.
- Enables the execution of software that makes significant system or security changes.
- Can make changes to the operating system.
- Can create new accounts.
- Can change the privileges of existing accounts.

The school will consider using multi-factor authentication, particularly for accounts that have access to sensitive or personal data.

The ICT technician will review the password system to ensure it is working at the required level.

8. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. The school will inform all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with the school's Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to Executive Headteacher and designated adults. Alerts will also be sent for unauthorised and accidental access. Alerts will identify the user, the activity that prompted the alert, and the information or service the user was attempting to access.

All incidents will be responded to in accordance with the 'Data security breach incidents' section of this policy, and as outlined in the Online Safety Policy.

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 accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the 'Data security breach incidents' section of this policy.

All data gathered by monitoring usage will be kept in the safeguarding file in the office of each school 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. In addition, the data may be used to ensure the school is protected and all software is up-to-date.

9. Removable media controls

The school understands that pupils and staff may need to access the school network from outside the school 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 and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Before distributing any school-owned devices, the ICT technician will ensure that manufacturers' default passwords have been changed. A set password will be chosen, and the staff member will be prompted to change the password once using the device. The ICT technician will check school-owned devices to detect any unchanged default passwords.

When using laptops, tablets and other portable devices, the Executive headteacher will determine the limitations for access to the network, as described in the 'Network security' section 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 the school premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any school-owned laptops, tablets or other devices, or when accessing school networks.

The online safety officer will use encryption to filter the use of websites on school-owned devices in order to prevent inappropriate use and external threats which may compromise 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 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 agreed prior to usage.

10. Home working and remote learning

Staff and pupils will adhere to data protection legislation and the school's related policies when working remotely.

Staff will receive annual training regarding what to do if a data protection issue arises from any home working or remote learning.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff and pupils may be required to use their own devices for the duration of the remote working or learning period. Any user on a personal device will need to access the school system through a proxy, e.g. VPN. Using a shared personal or household device for school purposes should be avoided where possible; however, the school understands that this may not always be possible.

Staff and pupils are not permitted to let their family members or friends use any school equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with the Disciplinary Policy and Procedure. This may also result in a data breach that the school would need to record and potentially report to the Information Commissioner's Office (ICO).

Staff who require access to personal data to enable them to work from home will first seek approval from the Executive headteacher, and it will be ensured that the appropriate security measures are in place by the ICT technician and the DPO, e.g. secure passwords and anti-virus software.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, **the device should be locked**. Where staff are using a personal device, they will be advised that a similar function should be implemented.

Personal data should not be transferred to a home device (such as a memory/data stick). When sending confidential information, staff must never save confidential information to a personal or household device. Data that is transferred from a work to a home device will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the school premises to allow staff to work from home, it should be transported in a lockable bag or container. The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

Staff will be expected to exercise particular vigilance when using school ICT equipment outside the workplace. Appropriate precautions will be taken, as required from time to time, to prevent the importation of viruses or the compromise of system security.

The system may contain information that is confidential and/or subject to data protection legislation. Such information will be handled with the utmost care and in strict accordance with the school's Data Protection Policy.

All staff working remotely will be required to comply fully with this policy and the Data Protection Policy at all times.

Staff should avoid taking physical copies of data, e.g. paper documents, off school premises unless absolutely necessary, such as when a digital version of the data does not exist. When taking physical copies of data off the school premises, staff will sign out the documents at the school office. The physical data will be signed back in when staff return it.

Pupils will not be permitted to use school-owned devices or software for activities that do not pertain to their online education, e.g. use of social media, gaming, streaming or viewing content that is not applicable to their curriculum. Pupils will also not be permitted to download any software onto school devices, unless instructed to and approved by their teacher.

Pupils will not alter the passwords or encryptions protecting school documents and systems put in place by the school. Pupils will not alter or disable any security measures that are installed on school devices, e.g. firewalls, malware prevention or anti-virus software. Pupils will not share any confidential and/or personal information made accessible to them, e.g. VPN passwords, with anyone who is not authorised to view that information.

Pupils that do not use school devices or software in accordance with this policy will be disciplined in line with the Behaviour Policy.

Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact the online safety officer if they wish to report any concerns regarding online safety.

Any devices that are used by staff and pupils for remote working and learning will be assessed by the ICT technician prior to being taken to the home setting, using the following checks:

- System security check – the security of the network and information systems
- Data security check – the security of the data held within the systems
- Online security check – the security of any online service or system, e.g. the school website
- Device security check – the security of the personal device, including any 'bring your own device' systems

The ICT technician will provide staff and pupils with details and instructions for accessing the school network that they will be using throughout the duration of the remote working and learning period.

In the event that a staff member or pupil decides to leave the school permanently, all data in any form will be returned on or before their last day. The ICT technician will then ensure that the said staff member or pupil no longer has access to the school network.

11. Backing up data

The ICT technician will perform a back-up of all electronic data held by the school on a termly basis, and the date of the back-up is recorded using a log. Each back up will be retained for as long as is necessary in accordance with Data Protection law before being deleted. The ICT technician will perform an incremental back-up on a monthly basis of any data that has changed since the previous back-up. The ICT technician will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

The ICT technician will ensure that there are at least three backup copies of important data, on at least two separate devices – one of which will remain off-site, e.g. cloud backups. The school will ensure any cloud servers used for backups encrypt this data to the state-of-the-art encryption standard, and all required data protection agreements are in place between the school and the cloud service provider.

The number of devices with access to back up data will be kept to an absolute minimum.

The school will follow the NCSC's guidance on backing up data where necessary, including:

- Identifying what essential data needs to be backed up.
- Storing backed-up data in a separate location to the original data.
- Considering using cloud solutions to store backed-up data.
- Referring to the NCSC's Cloud Security Guidance.
- Ensuring that backing up data is regularly practised.

The school will keep under review where servers can be replaced with cloud solutions, including accessing files, documents and shared folders. Where cloud solutions are used, the school will confirm its ICT provider ensures that data is portable and allows for:

- Secure encrypted transfer using a state-of-the-art encryption standard such as AES 256.
- Data export to an open standard or commonly used format.
- Data links through secure, documented application programming interfaces (APIs).
- A timely process for data transfer in an open standard or neutral format if the school ends the contract.
- Easy and secure access from a range of devices.

Where possible, back-ups will take place overnight and be completed before the beginning of the next school day. Upon completion of back-ups, data will be stored on the school's password protected hardware. Data will be replicated and stored in accordance with the school's Data Protection Policy. Only authorised personnel will be able to access back-ups of the school's data.

The school will ensure that offline or 'cold' back-ups are secured. This will be done by only digitally connecting the back-up to live systems when necessary, and never having all offline back-ups connected at the same time.

The school's back-up strategy will be tested on a monthly basis. All testing will be recorded.