Mayfield House School

Data and Cyber-security Breach Prevention and Management Plan

This Policy was last reviewed : 07 October 2026

Signed by:			
Mike Williams	Headteacher	Date:	07 October 2026
Martyn Deakin	Proprietor/Director	Date:	07 October 2026
Jacklyn Deakin	**Proprietor/Director**	**Date:**	**07 October 2026**

Last updated: 07 October 2026

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
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. Data security breach incidents
15. Assessment of risks
16. Consideration of further notification
17. Evaluation
18. Monitoring and review

Appendix A – Immediate Incident Response Checklist

Statement of intent

Mayfield House School is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible by the appropriate individuals. It is, therefore, important to uphold high standards of security, take suitable precautions, and to 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.

The school recognises that cyber security is intrinsically linked to safeguarding. Effective filtering, monitoring, access controls and data protection arrangements form part of the school's safeguarding framework in line with Keeping Children Safe in Education (as amended). Any cyber incident will be assessed for safeguarding implications and referred to the DSL where appropriate.

1. Legal framework

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

- UK General Data Protection Regulation, as amended.
- Data Protection Act 2018, as amended.
- Data (Use and Access) Act 2025, insofar as its provisions are in force and applicable.
- Computer Misuse Act 1990.
- Education (Independent School Standards) Regulations 2014, particularly Parts 3 and 8.
- Department for Education, Keeping Children Safe in Education 2026.
- Department for Education, Meeting digital and technology standards in schools and colleges, including the current cyber security and filtering and monitoring standards.
- Current Information Commissioner's Office guidance on data security, personal data breaches, monitoring and complaints.
- Current National Cyber Security Centre guidance on cyber security, authentication, phishing, ransomware and backups.
- Current Ofsted inspection toolkit and operating guidance for non-association independent schools.

This policy operates in conjunction with the following school policies:

- Online Safety Policy.
- Data Protection Policy.
- Disciplinary Policy and Procedure.
- Behaviour Policy.
- Social Media Policy.
- Remote Education Policy.
- Safeguarding and Child Protection Policy.
- Records Management and Retention Policy.
- Staff ICT and Electronic Devices Policy.
- Acceptable Use Policy.
- Business Continuity Plan.
- Complaints Policy, including data protection complaints arrangements.

Lawful processing and data minimisation

The school processes personal data lawfully, fairly and transparently in accordance with UK GDPR.

Personal data is:

- Collected for specified, explicit and legitimate purposes.
- Limited to what is necessary.
- Kept accurate and up to date.
- Retained only for as long as necessary.

The Data Protection Lead maintains the school's Record of Processing Activities. It is reviewed annually and updated when systems, providers or processing activities change. The school identifies the lawful basis for processing personal data and any additional condition required for special category or criminal offence data. Detailed arrangements are set out in the Data Protection Policy.

New systems, monitoring tools and significant changes to the use of personal data must be assessed before implementation. A data protection impact assessment will be completed where processing is likely to result in a high risk to individuals. Personal or confidential school information must not be entered into unapproved applications, artificial intelligence tools or personal accounts.

Data protection complaints will be handled through the school's published complaints arrangements. Complaints will be acknowledged within 30 days, investigated appropriately without undue delay, and complainants kept informed and told the outcome. This process does not replace immediate incident reporting or statutory breach notification.

2. Types of security breach and causes

A personal data breach is a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It may affect confidentiality, integrity or availability. Examples include a misdirected email, a lost paper file, unauthorised access, accidental deletion or ransomware preventing access to records. A cyber incident may require action even where no personal data breach has occurred.

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 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.

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 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 back-up copies of data, meaning the most recent data could be overwritten.

3. Roles and responsibilities

The Proprietors (Directors) retain ultimate strategic responsibility for cyber security, data protection and information governance.

They will:

- Receive termly reports on cyber security, filtering and monitoring effectiveness.

- Ensure cyber risks are included in the school's strategic risk register.
- Ensure sufficient financial and staffing resources are allocated to maintain secure systems.
- Ensure compliance with UK GDPR, ISSR and safeguarding requirements.
- Undertake appropriate cyber security awareness training.

Cyber security forms part of routine proprietor oversight meetings.

The company operating Mayfield House School retains responsibility for its obligations as data controller. Commissioning external IT services does not transfer that accountability.

The Data Protection Lead is responsible for:

- Coordinating the school's data protection procedures and records of processing.
- Advising staff on secure handling of information.
- Coordinating personal data breach assessments and maintaining the breach register.
- Arranging ICO and individual notifications where required.
- Checking relevant supplier data protection arrangements.
- Coordinating training with the Headteacher and IT support.
- Seeking specialist advice where necessary.
- Reporting significant issues and outstanding actions to the Proprietors.
- Reviewing this plan with the Headteacher, DSL and IT support.

The school has assessed its processing activities and concluded that a statutory Data Protection Officer appointment is not required. The assessment is retained and will be reviewed if the nature or scale of processing changes.

"IT support" includes commissioned providers and authorised internal personnel. The school maintains a written allocation of responsibilities for devices, networks, cloud systems, backups, filtering and monitoring, account administration and technical incident response.

The IT support is 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 premises.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Installing, monitoring and reviewing filtering systems for the school's network.
- Setting up user privileges in line with recommendations from the headteacher.
- Maintaining an account and permissions register and secure password-reset procedures, without routinely retaining users' passwords.
- Removing any inactive users from the school's system, ensuring that this is always up-to-date.
- 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.
- Ensuring all school-owned devices have secure malware protection and that devices are regularly updated.
- Recording relevant filtering and monitoring alerts and promptly notifying the DSL or deputy where there is a safeguarding concern. Immediate risks of harm must be escalated immediately. Technical security concerns are referred to the digital lead and suspected personal data breaches to the Data Protection Lead.

The online safety officer is 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.
- Liaising with the LA where appropriate.
- 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 Data Protection Lead.
- 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 Data Protection Lead and IT support.

The headteacher is 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 Data Protection Lead.
- Ensuring a log of cyber-security incidents is maintained.
- Maintaining a proportionate incident response group comprising the designated digital lead, Headteacher, DSL, Data Protection Lead and IT support, with deputies and additional specialists where required.

The Proprietors will designate a Director or senior leader as the digital lead. Responsibilities may be combined where appropriate to the school's size and available expertise.

The designated digital lead is responsible for:

- Identifying and evaluating the school's most significant cyber risks.
- Recording historical incidents to inform future mitigation strategies.
- Monitoring user behaviour to highlight risks that may compromise cyber security.
- Working in conjunction with IT support to:
- Establish a clear reporting and escalation process for cyber risks.
- Integrate cyber risks into the school's risk register and business continuity plan, with regular testing.
- Maintain response and recovery arrangements consistent with the school's actual commercial insurance conditions.
- Notify directors of material risks as part of routine strategic reporting.
- Working in conjunction with the **Data Protection Lead** to:
- Complete and maintain a Record of Processing Activities (ROPA) for all systems processing personal or sensitive data.
- Assess staff access levels and permissions and verify the adequacy of password policies.
- Ensure email security is configured to mitigate risks from spoofed or imitation emails.

Current role holders, deputies, provider responsibilities and emergency contacts are maintained in a restricted directory accessible during a school-system outage.

The DSL will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security 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.

- Following IT support instructions, making devices available for updates and reporting security warnings promptly. Staff must not install unapproved software or alter security settings.

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. This will be stored in the **school office** and will be audited on a **termly** basis to ensure it is up-to-date.

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

IT support manages security updates throughout the year. Critical or high-risk vulnerability fixes, fixes with a CVSS score of 7.0 or above, and fixes without a vendor severity rating will be completed within 14 days of release. Other updates will be prioritised according to risk. Urgent threats may require earlier action. Termly audits check compliance and do not replace ongoing updates.

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 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 where compromise is suspected or identified, and password strength requirements are enforced at system level in line with NCSC guidance.

The school believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

Password requirements will follow current NCSC guidance and system capabilities. Passwords must be unique, resistant to guessing and protected against unauthorised access. Common or compromised passwords will be blocked where supported. Passwords must be changed where compromise is suspected or confirmed.

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** – Access is limited to authorised users according to their role. The school currently uses password-based authentication. IT support will implement MFA for relevant staff cloud accounts, remote access and administrator accounts. Coverage, exceptions and interim controls are recorded as described in the User privileges section.
- **Malware protection** – The school will protect itself from malware by installing antivirus and anti-malware software, and using techniques such as whitelisting (a cyber-security strategy under which a user can only take actions on their computer that an administrator has explicitly allowed in advance) and sandboxes (an isolated virtual machine in which potentially unsafe software code can execute without affecting network resources or local applications).
- **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.

IT support 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.

- Restrict firewall administration to authorised personnel. IT support will confirm and document authentication controls, MFA availability and permitted remote access, and address any identified weaknesses.
- 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.

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.

Network protection and safeguarding oversight

The school commissions external IT support and uses Netsweeper as part of its filtering arrangements. The digital lead maintains a verified record of products, services, licences, settings and responsibilities at both sites.

Firewall protection, web filtering, malware protection and safeguarding monitoring are separate functions. The school obtains confirmation of the functions provided, including device and off-site coverage, alerts, reports and limitations.

The responsible senior leader, supported by the DSL and IT support, reviews filtering and monitoring effectiveness at least annually. Termly assurance checks and additional reviews following significant changes or incidents are recorded. Checks cover relevant devices and locations at both sites.

Filtering and monitoring reflect pupils' ages, SEND and vulnerabilities without unnecessarily restricting learning or accessibility tools.

Safeguarding concerns reach the DSL or deputy promptly, with immediate escalation where harm may be imminent. Technical threats reach IT support. Alert-review responsibilities, absence cover and out-of-hours arrangements are documented.

The Proprietors receive termly assurance on checks, significant incidents, weaknesses and actions.

Supplier responsibilities

The school maintains written responsibilities for I-Tech MF and other relevant providers. Compliant processor contracts are required where providers process personal data on the school's behalf. Arrangements address confidentiality, security, subcontractors, incident notification, recovery assistance and data return or deletion. Applicable international-transfer requirements must be met.

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 IT support 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.

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

Unsupported technology is replaced or removed from service. Temporary exceptions require a documented risk assessment, appropriate isolation and compensating controls, an owner and an approved replacement deadline.

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.

IT support ensures appropriate malware protection is active and updated automatically. Failures and significant alerts are investigated promptly. Termly assurance reviews check coverage, update status and outstanding risks.

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, as described in the Network security section, will ensure that access to websites with known malware are blocked immediately and reported to the IT support.

IT support maintains appropriate email security controls to reduce the risk of malware, spam and phishing reaching users. These controls cannot identify every threat. Updates and significant alerts are managed throughout the year, with coverage and effectiveness checked termly. Staff must remain vigilant and report suspicious messages promptly.

Staff may install applications on school-owned devices only through approved sources and with school authorisation under the agreed IT arrangements. IT support manages security updates. Staff must follow IT support instructions, make devices available for updates and must not install unapproved software or alter security settings.

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.

7. User privileges

Access is authorised according to role and limited to what each user needs. IT support maintains an account and permissions register without routinely recording users' passwords.

Staff use individual accounts. Administrator accounts must be individually attributable, restricted and separate from ordinary email and daily work. Emergency access is secured, limited and logged. Existing shared administrator arrangements must be assessed and replaced with individually attributable access.

The school currently uses password-based authentication and has confirmed that MFA can be introduced. IT support will agree and implement a rollout for staff cloud accounts, remote access and administrator accounts. Completion must be verified before the school records MFA as operational.

Until implementation, strong unique passwords, appropriate access restrictions and monitoring will be maintained. Any system limitations, exceptions and interim controls are recorded in the cyber risk assessment with an owner and review date.

Pupil access reflects age, understanding and SEND. Staff support secure authentication and password resets where necessary. Pupils must not receive administrator privileges or access to confidential records.

Visitors use segregated guest internet access. Access to school systems requires specific authorisation and appropriate time limits.

HR and line managers notify IT support promptly of joiners, role changes and leavers. Access is disabled when no longer authorised, including active sessions and remote access. Records are preserved under the retention policy before account deletion. Shared mailboxes are accessed through authorised individual accounts.

Permissions are reviewed termly and after relevant changes. Automated administration may be used where suitable.

8. Monitoring usage

Monitoring has specified safeguarding and security purposes and must be necessary and proportionate. Staff, pupils and parents receive appropriate information through privacy notices and acceptable use arrangements, with accessible explanations for pupils.

Monitoring is assessed before implementation. A data protection impact assessment is completed where processing is likely to create high risk.

Safeguarding concerns are escalated directly to the DSL or deputy. Technical threats reach IT support and the digital lead. Suspected personal data breaches also reach the Data Protection Lead.

Logs and reports are held securely with restricted access and retention periods set under the Records Management and Retention Policy. Relevant investigation evidence is preserved.

Records show significant alerts, actions and outstanding issues. An alert alone is not proof of misconduct.

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.

Portable school devices containing personal or confidential information use appropriate encryption, access controls and device management. Removable storage requires authorisation, appropriate encryption and malware checks. Encryption reduces disclosure risk but loss or theft must still be reported immediately.

Before distributing any school-owned devices, the IT support will ensure that manufactures' 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 IT support will check school-owned devices on a termly basis to detect any unchanged default passwords.

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. 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 support.

When using laptops, tablets and other portable devices, the headteacher will determine the limitations for access to the network, in accordance with the User privileges section.

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 use approved connectivity and remote-access arrangements away from school. Devices retain their security controls. Filtering, secure connections and encryption perform different functions. Tracking or remote wiping may be used where authorised, proportionate and supported.

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

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.

School-managed devices are preferred for remote access to confidential information. Personal devices require authorisation and assessment of security, privacy and safeguarding risks. Approved access may use secure cloud services or a VPN according to the system. A VPN alone does not make a device secure.

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. Suspected unauthorised disclosure will be investigated and addressed fairly under the relevant school procedures. This may also result in a data breach that the school would need to record and potentially report to the ICO.

Staff members who require access to personal data to enable them to work from home will first seek approval from the headteacher, and it will be ensured that the appropriate security measures are in place by the IT support and the Data Protection Lead, 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.

School devices will automatically lock after **one minute** of inactivity to avoid an unauthorised person gaining access to the device. Where staff are using a personal device, they will be advised that a similar function should be implemented.

Staff access personal data through approved systems. Personal or household devices must not retain confidential school information. Necessary local storage requires specific authorisation and must be confined to a secured school-managed device with defined deletion arrangements.

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

- 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 house members can access personal data
- Using an unsecured Wi-Fi network

Staff working from home will be encouraged 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 will be transported in a lockable bag or container. This will apply to data that is both paper-based and electronic.

When taking physical copies of data, e.g. paper documents and school-owned devices, 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 are not 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 are not 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.

Concerns about pupil use are addressed through safeguarding, teaching and the Behaviour Policy, considering age, SEND, understanding and reasonable adjustments. Deliberate misuse may result in proportionate action following assessment.

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 IT support 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 IT support should provide staff and pupils with details and instructions for accessing the school's network that 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.

11. Backing-up data

The digital lead and IT support maintain a documented backup and recovery plan covering essential information and systems, including cloud services.

The plan identifies what is protected, responsible providers, backup frequency, retention, recovery priorities, maximum acceptable data loss and target restoration times.

Critical changing records should be protected at least daily, or through an equivalent verified provider arrangement meeting the school's recovery needs. More frequent protection is used where required. Gaps are risk-assessed, assigned an owner and addressed within an agreed timescale.

Three copies of essential data are maintained overall, including the working copy, across two separate media or devices, with one off-site. Arrangements include protection against attacker deletion or encryption.

IT support monitors completion and investigates failures. Cloud synchronisation and general disaster-recovery statements are not assumed to provide adequate backups.

Restoration tests are completed and recorded monthly, demonstrating that selected records can be restored and used. The plan is reviewed annually and after significant changes or incidents.

Backup retention is documented separately from live-record retention. Restored information is brought into line with current retention and access requirements.

12. Avoiding phishing attacks

The IT support will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as many rights as are required to perform their jobs.

Administrator accounts must not be used for routine email or browsing. Staff use ordinary individual accounts for daily work. Authentication arrangements follow the User privileges section.

In accordance with the User training and awareness section, the Data Protection Lead and headteacher will organise regular training for staff members – this will cover identifying irregular methods of communication 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. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

Staff will use the following warning signs when considering whether a communication may be unusual:

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

Fraudulent messages may be well written and come from compromised genuine accounts. Familiar names or logos do not establish authenticity. Supplier bank-detail changes and unusual payments must be verified through an independently established contact method, rather than details supplied in the message.

The IT support will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, managed in accordance with the Network security and Malware prevention sections. The IT support will ensure that the filtering system is neither too strict nor too lenient, to allow the correct emails to be sent to the relevant folders.

To prevent anyone having access to personal, unnecessary information, the Data Protection Lead will ensure the school's social media accounts and websites are reviewed on a **termly** basis, making sure that only necessary information is shared.

The headteacher and Data Protection Lead will ensure the school's Social Media Policy includes expectations for sharing of information – and determines what is and is not appropriate to share.

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, in accordance with the school's Acceptable Use Policy.

13. User training and awareness

The Data Protection Lead and headteacher will arrange training for pupils and staff on a **termly** basis to ensure they are aware of how to use the network appropriately, in accordance with the Acceptable Use Policy. This will cover identifying irregular methods of communication 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. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

The online safety officer will arrange for staff and pupils to undertake the appropriate training relating to online safety issues.

The Data Protection Lead will also arrange training for pupils and staff on a **termly** basis maintaining data security, preventing data breaches, and how to respond in the event of a data breach. Training for all staff members will be arranged by the online safety officer and Data Protection Lead within **two weeks** following an attack, breach or significant update.

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.

Staff with access to the school's IT network will be required to undertake basic cyber-security training upon induction which is refreshed every year. The Proprietors will also undertake appropriate cyber security awareness training. The training will focus on the following:

- Phishing
- Password security
- Social engineering
- The dangers of removable storage media

Users will understand acceptable use and reporting expectations. Suspected misuse will be assessed fairly under the relevant school procedures, taking account of pupil SEND and safeguarding needs.

Pupil teaching is adapted to age, understanding, SEND and communication needs. Training completion and outstanding actions are recorded.

14. Data security breach incidents

Suspected cyber incidents or personal data breaches must be reported immediately to the Headteacher or deputy and Data Protection Lead. IT support must be contacted for technical incidents. Safeguarding concerns also reach the DSL or deputy immediately. Reporting must not wait until the next working day. Emergency contacts are held in the incident directory.

When an incident is raised, the Data Protection Lead 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
- Whether the incident needs to be reported to the relevant authorities, e.g. ICO or the police
- Time of discovery and when the school became aware of the breach.
- Containment actions, notification decisions and deadlines.
- Reasons for reporting or not reporting, recovery actions and outstanding tasks.

The school's Data Protection Lead will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this. The Data Protection Lead, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or has been compromised. The Data Protection Lead will oversee a full investigation and produce a comprehensive report.

The cause of the breach, and whether it has been contained, will be identified – ensuring that the possibility of further loss or jeopardising of data is eliminated or restricted as much as possible.

If the Data Protection Lead 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.
- Disciplinary action is not automatic. Facts, training, system weaknesses and conduct will be assessed fairly. Pupil responses consider SEND and safeguarding. Prompt reporting is encouraged.

- The Data Protection Lead records the incident, coordinates the personal data risk assessment and documents notification decisions. IT support carries out necessary technical containment and recovery actions, including access restrictions, password resets and changes to security controls. Evidence and existing backups must be preserved; affected data must not be copied or restored without IT advice.
- The school will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.
- The school will organise updated staff training following a breach.
- 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.

Where the security risk is high, the Data Protection Lead 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.
- Preserving evidence and existing backups, and obtaining IT advice before copying or restoring affected data.
- 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.

The school notifies the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to risk individuals' rights and freedoms. Decisions are recorded. Delayed notifications explain the delay. Information may be provided in phases without undue further delay.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours. The information required can be provided in phases, as long as this is done without undue further delay.

In line with the UK GDPR, the following must be provided to the ICO when reporting a personal data breach:

- A description of the nature of the breach, including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Lead
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects, where appropriate

Schools will report a personal data breach to the ICO via their website. The school will also make use of the ICO's self-assessment tool to determine whether reporting a breach is a necessary next step.

Where a breach is likely to create high risk to individuals' rights and freedoms, affected individuals are informed without undue delay, subject to Article 34 exceptions. Accessible communication explains the breach, consequences, protective measures and contact point.

The response group coordinates relevant police or Report Fraud reports and any DfE, NCSC, insurer or contractual notifications.

IT support verifies that systems are safe before reconnection. The response group authorises restoration of normal operations, considering safeguarding and continuity. Recovery actions and unresolved risks are recorded.

15. Assessment of risks

As a small independent SEN school, the school recognises that many pupils may be more vulnerable to online manipulation, exploitation or coercion. Cyber security measures are therefore designed not only to protect systems, but also to protect vulnerable pupils from safeguarding harm.

The following questions will be considered by the Data Protection Lead 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 Data Protection Lead's report, which should record:

- What type of, and how much, data is involved?
- Does it include special category data, criminal offence data or other confidential information? Consider health, clinical, safeguarding, EHCP, care-status, financial and protected contact information.
- 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 data has been compromised, are there effective measures to reduce its impact, such as verified recoverable backups?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, proprietors, 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.
- Exposure to abuse, exploitation, coercion or unwanted contact.
- Loss of information needed for safe medication, safeguarding, attendance or authorised-carer communication.
- 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 LA, external partners, authorities, or others provide effective support?
- Does the breach need to be reported to the ICO? If so, has it been successfully reported without undue delay?

The school will ensure that a cyber risk assessment is conducted annually and reviewed every term. This risk assessment will be used to:

- Understand how to keep pupils, staff and the wider school community safe.
- Understand how prepared the school is in response to a cyber incident or attack.
- Highlight weaknesses and put processes in place to help reduce risk.
- Secure systems to ensure resilience against cyber incidents and attacks.
- Prepare a cyber response plan to be implemented quickly in the event of a serious incident to minimise any impact to the school.
- Avoid safeguarding issues, disruption, significant data breaches, reputational damage or significant unexpected spend and lost staff time to recover systems and data.

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

16. Consideration of further notification

The Data Protection Lead 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 data security.

The Data Protection Lead will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password. ICO and individual notifications follow the thresholds in the Data security breach incidents section. A breach affecting one vulnerable pupil may require notification.

The Data Protection Lead 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.
- 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.

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

17. Evaluation

The Data Protection Lead will document all the facts regarding the breach, its effects and the remedial action taken. This should be an evaluation of the breach, and what actions need to be taken forward.

The Data Protection Lead will consider the data and contexts involved, establish the root of the breach, and where any present or future risks lie, taking into consideration whether the breach is a result of human or systematic error and see how a recurrence can be prevented.

The Data Protection Lead and headteacher will identify any weak points in existing security measures and procedures. The Data Protection Lead will work with the IT support to improve security procedures wherever required. The Data Protection Lead and headteacher will identify any weak points in levels of security awareness and training.

The Data Protection Lead will report on findings and implement the recommendations of the report after analysis and discussion.

Improvement actions have an owner, deadline and completion record. The Proprietors oversee significant findings and outstanding risks.

18. Monitoring and review

This plan is reviewed annually by the Headteacher and Data Protection Lead, with input from the DSL, digital lead and IT support, and approved by the Proprietors. Earlier review follows significant incidents, changes to systems or providers, or relevant legal and guidance changes.

The Proprietors receive termly assurance on significant risks, access reviews, filtering checks, backups, restoration tests, training and outstanding actions.

Emergency contacts are checked termly and updated following changes. Incident response arrangements are exercised annually, with findings recorded.

Next scheduled review: 07 October 2027.

Appendix A Immediate Incident Response Checklist

1. Report immediately and record discovery time.
2. Contact the DSL or deputy where anyone may be at risk.
3. Follow IT isolation instructions. Do not wipe, delete or reconnect without authorisation.
4. Preserve relevant evidence securely.
5. Use alternative communication if normal systems are compromised.
6. Maintain safe attendance, medication, safeguarding and emergency-contact arrangements at both sites.
7. Record breach awareness time, risk assessment and notification deadlines.
8. Contact providers and insurers as appropriate.
9. Restore services using verified safe systems and data.
10. Authorise normal operation and record follow-up actions.

A restricted emergency directory accompanies this checklist and remains accessible during a system outage. It identifies role holders, deputies, providers, insurers, reporting routes and alternative communication arrangements.