

Cyber-Security Policy



Review body: Compliance Governor

Date policy last reviewed: 09/02/2026

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 and passwords
8. Monitoring usage
9. Removable media controls and home working
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 and response
18. Monitoring and review

Appendix

1. Roles and Responsibilities
2. School network user privileges

Statement of intent

Coldean Primary School is 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. In schools, most breaches are caused by human error, so 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.

This policy is based on a model from The National College, last updated 02/09/2025.

1. Legal framework

1.1. This policy has due regard to statutory legislation and advisory 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'

1.2. This policy has due regard to the school's policies and procedures including, but not limited to, the following:

- Online Safety Policy
- Data Protection Policy
- Behaviour Policy
- Social Media Policy
- Remote Education Policy
- Cyber Response and Recovery Plan

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. 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.
- 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:
- 2.5.1. Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- 2.5.2. 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.

2.5.3. 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.

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
- Operational errors, such as confusion between backup copies of data, meaning the most recent data could be overwritten.

3. Roles and responsibilities

3.1. The governing board will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school has an appropriate approach to managing data breaches in place.
- Supporting the 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.

3.2. 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 DPO.
- Ensuring a 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.

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

- The
- 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.
- Assessing the risks to the school in the event 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 **online safety officer, headteacher and IT Technician** after a data security breach to determine where weaknesses lie and improve security measures.

- Monitoring the effectiveness of this policy, alongside the **online safety officer** and **headteacher**, and communicating any changes to staff members.

3.4. The **ICT technician** will be responsible for:

- Ensuring any out-of-date software is removed from the school systems.
- 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 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 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 are regularly updated.
- Recording any alerts for access to inappropriate content and notifying the headteacher.

3.5. The **online safety officer** is responsible for:

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

3.6. 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.

3.7. **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

4. Secure configuration

- 4.1. 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 is in secured cloud storage on OneDrive accessible by online safety officer, Business Manager and IT Technicians. This is audited on an **annual** basis to ensure it is up-to-date.
- 4.2. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the **online safety officer** before use.
- 4.3. All systems will be audited on a **termly** basis by the **online safety officer** and **IT 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.
- 4.4. 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.
- 4.5. All hardware, software and operating systems will require passwords from individual users before use. Passwords will be changed on an **annual** basis to prevent access to facilities which could compromise network security.
- 4.6. 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. Passwords will need to adhere to a specific character length, use special characters, and not be obvious or easy to guess, in line with the school's policy on passwords.

The school and its ICT providers (BHCC) refers to the five security controls outlined in the National Cyber Security Centre's (NCSC's) ['Cyber Essentials'](#). These are:

1. **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.
2. **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.
3. **Access control** – The more people have access to data, the larger the chance 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, two-factor authorisation.
4. **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).
5. **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 (MFA), 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.

5. Network security

- 5.1. In line with the UK GDPR, the school will appropriately test, assess, and evaluate any security measures put in place on a regular basis to ensure these measures remain effective.
- 5.2. The school's firewall is deployed as a centralised deployment, which means the broadband service connects to a firewall that is located within a data centre or other major network location.
- 5.3. 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.
- 5.4. 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.
- 5.5. 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.
- 5.6. 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.

- 5.7. Unlicensed hardware or software will never be used by the school.
- 5.8. 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.

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 **IT technician** will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements.
- 6.3. The **IT technician** will ensure that malware protection is updated on a **termly** 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. 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
- 6.6. 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.
- 6.7. Filtering of websites will ensure that access to websites with known malware are blocked immediately and reported to the ICT technician.
- 6.8. 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.
- 6.9. Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the online safety officer. 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.
- 6.10. 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

- 7.1. 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.
- 7.2. The **headteacher** will clearly define what users have access to and will communicate this to the **IT technician**, ensuring that a written record is kept.
- 7.3. The **IT technician** will ensure that user accounts are set up to allow users access to the facilities required, in line with the **headteacher's** instructions, whilst minimising the potential for deliberate or accidental attacks on the network.
- 7.4. All staff users will be required to change their passwords on an annual basis and/or if they become known to other individuals, in line with the 'Secure configuration' section of this policy.
- 7.5. The **online safety officer** will have an up-to-date record of all pupil usernames and passwords and will be able to reset them if necessary. The record of all pupil usernames and passwords is encrypted.
- 7.6. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible.
- 7.7. The 'master user' password used by the ICT technician will be made available to the headteacher and online safety officer.
- 7.8. 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.
- 7.9. The ICT technician in liaison with the online safety officer will delete inactive users or users who have left the school at a school network level, i.e. *active directory*
- 7.10. The online safety officer is responsible for the deletion of inactive users or users that have left the school at a portal level, e.g. *school email, online assessment, MIS access*.
- 7.11. 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.
- 7.12. The school will implement a user account creation, approval and removal process which is part of the school joining and leaving protocols.
- 7.13. 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.
- 7.14. The school uses multi-factor authentication for staff email accounts and any others that have access to sensitive or personal data and is available.
- 7.15. The ICT technician will review the password system on a termly basis to ensure it is working at the required level.

8. Monitoring usage

- 8.1. Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.
- 8.2. The school will inform all pupils and staff that their usage will be monitored, in accordance with the school's **Online Safety Policy**.
- 8.3. If a user accesses inappropriate content or a threat is detected, an alert will be sent to the **online safety officer**. Alerts will also be sent for unauthorised and accidental usage. Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.
- 8.4. The **online safety officer** will record any alerts using an incident log and will report this to the **headteacher**. 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**.
- 8.5. 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.
- 8.6. All data gathered by monitoring usage will be kept in a locked filing cabinet on a shared drive 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

- 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 **IT Technician** will encrypt all school-owned devices for personal use, such as laptops and tablet devices, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.
- 9.3. Before distributing any school-owned devices, the **IT 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.
- 9.4. When using laptops, tablets and other portable devices, the **headteacher** will determine the limitations for access to the network, as described in 'Network security' section of this policy.
- 9.5. 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.
- 9.6. The **online safety officer** will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.
- 9.7. The school uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.
- 9.8. 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.

- 9.9. The Wi-Fi network at the school is password protected.
- 9.10. Restricted access to the Wi-Fi network is available via a Guest Pass. Passes are allocated only for the required duration. Only the **IT Technicians** and the **online safety officer** are able to allocate passes. Access is limited to Internet only.

10. Home working and remote learning

- 10.1. Staff and pupils will adhere to data protection legislation and the school's related policies when working remotely.
- 10.2. Staff will receive annual training regarding what to do if a data protection issue arises from any home working or remote learning.
- 10.3. 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.
- 10.4. Staff may be required to use their own devices for the duration of the remote working or learning period.
- 10.5. Access to documents is through a password protected cloud-share system, OneDrive.
- 10.6. 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 ICO.
- 10.7. Staff 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 ICT technician and the DPO, e.g. secure passwords and anti-virus software.
- 10.8. 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.
- 10.9. Personal data should only be transferred to a home device if this is necessary for the member of staff to carry out their role. 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.
- 10.10. 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.
- 10.11. 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 will 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.

10.12. 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.

10.13. 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.

10.14. 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.

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

10.16. 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.

10.17. 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

10.18. 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

11.1. The ICT technician performs a back-up of all electronic data held by the school on a daily basis, and the date of the back-up is recorded using a log. Each back-up is retained for three months before being deleted.

11.2. 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.

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

11.4. 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.

11.5. 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.
- 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.

11.6. Back-ups are run overnight and are completed before the beginning of the next school day. Upon completion of back-ups, data is stored on the school's hardware, which is password protected. 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.

11.7. The school will ensure that offline or 'cold' back-ups are secured. This can 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.

12. Avoiding phishing attacks

12.1. The **IT Technician** 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.

12.2. Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account. Two-factor authentication is used on any important accounts, such as the master user account, or any key accounts, such as the headteacher's or SBM's accounts.

12.3. 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?
- Is it from a supplier advising of a change in bank account details for 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.
- Is it from a generic email address, such as Gmail or Hotmail?

12.4. The **IT technician** will ensure that email filtering systems is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy.

12.5. The **ICT technician** 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

- 12.6. To prevent anyone having access to unnecessary public information, the **DPO** will ensure the school's social media accounts and websites are reviewed on a **termly** basis, making sure that only necessary information is shared.
- 12.7. The **headteacher** will ensure the school's Social Media Policy includes expectations for sharing of information and determines what is and is not appropriate to share.
- 12.8. 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.

13. User training and awareness

- 13.1. The **headteacher** will arrange training for pupils and staff on a regular basis to ensure they are aware of how to use the network appropriately in accordance with the **Acceptable Use Policy** and **Online Safety 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.
- 13.2. The **online safety officer** will arrange for staff and pupils to undertake the appropriate training relating to online safety issues.
- 13.3. The **DPO** will also arrange training for pupils and staff on a termly basis on 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 **DPO** within two weeks following an attack, breach or significant update.
- 13.4. 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.
- 13.5. 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. At least one member of the governing board will also take part in this training. The training will focus on the following:
 - Phishing
 - Password security
 - Social engineering
 - The dangers of removable storage media
- 13.6. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Behavioural Policy and the Disciplinary Policy and Procedure.

14. Cyber-security incidents

- 14.1. All cyber-security incidents will be managed in line with the school's Cyber Response and Recovery Plan.
- 14.2. Any individual that discovers a cyber-security incident will report this immediately to the online safety officer and the DPO.
- 14.3. 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
 - Whether the incident needs to be reported to the relevant authorities, e.g. the ICO or police
- 14.4. The school's DPO will take the lead in investigating the incident, with assistance from the online safety officer, and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the incident and determine if any personal data is involved or has been compromised.
- 14.5. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the incident, 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.
- 14.6. 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 who caused the breach, in accordance with the Behavioural Policy or Disciplinary Policy and Procedure
 - 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
- 14.7. Where the security risk is high, the DPO will establish what 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.
- 14.8. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.
- 14.9. Schools are required to report personal data breaches to the ICO if there is a likelihood of risk to people's rights and freedoms. If the DPO decides that risk is unlikely, the breach does

not need to be reported; however, the school will need to justify this decision and document the breach.

- 14.10. The DPO will notify the ICO within 72 hours of becoming aware of a breach where it is likely to result in a risk to the rights and freedoms of individuals.
- 14.11. 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.
- 14.12. 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 DPO
 - 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
- 14.13. The school will report a personal data breach via the ICO 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.
- 14.14. 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 without undue delay.
- 14.15. Where the school has been subject to online fraud, scams or extortion, the DPO will also report this using the Action Fraud website.
- 14.16. The DPO and ICT technician 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.

15. Assessment of risks

- 15.1. 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 LA**, external partners, authorities, or others provide effective support?

15.2. 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.

16. Consideration of further notification

- 16.1. 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.
- 16.2. 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.
- 16.3. If a large number of people are affected, or there are very serious consequences, the ICO will be informed.
- 16.4. 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.
- 16.5. The ICO will be consulted for guidance on when and how to notify them about breaches.
- 16.6. 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.

17. Evaluation

- 17.1. The **DPO** 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.
- 17.2. The **DPO** 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.
- 17.3. The **DPO** and **headteacher** will identify any weak points in existing security measures and procedures. The **DPO** will work with the **ICT technician** to improve security procedures wherever required. The **DPO** and **headteacher** will identify any weak points in levels of security awareness and training.
- 17.4. The **DPO** will report on findings and implement the recommendations of the report after analysis and discussion.

18. Monitoring and review

- 18.1. This policy will be reviewed by the **online safety officer**, in conjunction with the **DPO** on an **annual** basis. The next scheduled review date for this policy is **January 2027**
- 18.2. The **DPO** is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.

APPENDIX I

Roles and Responsibilities

Role	Responsibilities	Staff Member
Data Protection Officer	• Deal with freedom of information and subject access requests. • Ensure the school collects, processes, stores and destroys data in accordance with UK GDPR • Ensure a consent record is kept up-to date • Ensure Privacy Notices are compliant, up to date and shared • Ensure that where data is outsourced, the third parties uphold the same data protection standards as the school. • Report any breaches to the Information Commissioner's Office within the legal time frame.	Data Protection Education Ltd. https://dataprotection.education dpo@dataprotection.education 0800 0862018
Data Controller	Determine the purposes and means of processing personal data	Coldean Primary School
Data Manager	Monitors the school's action in collecting, processing, storing and destroying data in accordance with UK GDPR	Nigel Watson
Governor responsible for Compliance	• Ensuring the school has appropriate cyber-security measures in place. • Ensuring the school has an appropriate approach to managing data breaches in place. • Supporting the 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.	Becky Ouassa
Data Processor	Process data on behalf of the Data Controller	• Senior Leadership Team • Class teachers • Teaching Assistants • Individual Needs Assistants • Office Staff • Caretaker • Governors

Appendix II

School Network User Privileges

Coldean Primary School's server is organised by data security permissions.

RED_1 Personal/Sensitive data accessible by administration staff.

RED_2 Personal/Sensitive pupils' data accessible by teaching staff.

AMBER Personal and organisational data accessible by administration, teaching staff and support staff

GREEN Data accessible by all staff, trainee teachers and supply staff.

CHILDREN Data accessible by all staff, trainee teachers, supply staff and pupils.

The colour coding is to facilitate permission settings and also to remind staff of the need to restrict access for personal/sensitive data. If the data is on a RED drive it **must not** be copied onto AMBER or GREEN.

Headteacher (HT), Deputy Head (DHT), Assistant Head (AHT), SENDCo, Business Manager (SBM), Office Manager (OM), Office Admin (OA), Child Welfare Officer (CWO), Class Teacher (CT), Learning Mentor (LM), Teaching Assistant (TA), Individual Needs Assistant (INA)

RED_1	ACCIDENTS + INCIDENTS	HS2 and HS3 forms	HT, DHT, SBM, OM
	ADMISSIONS	For future admissions paperwork if required	HT, DHT, SBM, OM
	ATTENDANCE	For future attendance paperwork if required. Letters created and sent within SP	HT, DHT, OM, CWO
	BUSINESS MANAGER	Finance & Personnel	HT, SBM
	GOVERNORS		HT, DHT, CoG, Clerk to Govs
	INVENTORY		HT, DHT, SBM, OM, OA
	JOB VACANCIES		HT, DHT, SBM, OM
	OPERATION ENCOMPASS		HT, DHT, CWO
	PREMISES		HT, DHT, SBM, OM, Caretaker

	PUPIL ADMIN	Documents pertaining to general pupil admin e.g. <i>class lists, lunchtimes, parental consent etc.</i>	HT, DHT, SBM, OM, OA
	SAFEGUARDING AUDIT		HT, CWO
	SINGLE CENTRAL REGISTER		HT, DHT, SBM, CWO, OM
	SMT		HT, DHT, AHT, SENDCo, LKS2 lead, UKS2 lead
	SUPPLY	Spreadsheet of supply costs. Any documentation related to agencies.	HT, DHT, SBM, OM

RED_2	ASSESSMENT	Pupil assessment data	SLT, CTs
	DATA ANALYSIS		SLT, CTs
	END OF YEAR REPORTS		SLT, CTs
	INTERNAL TRANSFERS	End of year transfer notes	SLT, CTs
	LEARNING MENTORS		SLT, LMs, CWO
	PUPIL MEDICAL PLANS		SLT, CTs, LMs, TAs, INAs
	PUPIL PROGRESS MEETINGS		SLT, CTs
	SEN-D		SLT, LMs, CTs
	STAFF MEETING MINUTES		SLT, CTs, LMs, TAs, INAs
	STATUTORY ASSESSMENT	All DfE documentation i.e. ARAs; class lists/assessment records for EYFSP, Y1 Phonics, End KS1, Y4 Tables, End KS2.	SLT, CTs

	TRAINEE TEACHERS	Observation records and reports of trainee teachers.	SLT, CTS
--	------------------	--	----------

CHILD PROTECTION			HT, CWO, OM
-------------------------	--	--	-------------

AMBER	AFTER-SCHOOL CLUBS		SLT, CTs, SBM, OM, OA
	CLASS LISTS		SLT, CTs, OM, OA, TAs, INAs
	EDUCATIONAL VISITS		SLT, CTs, SBM, OM, OA
	HOUSE SYSTEM		SLT, CTs, TAs, INAs, OM, OA
	PHOTOS & VIDEOS		SLT, CTs, TAs, INAs, OM, OA
	SCHOOL COUNCIL		SLT, CTs

GREEN	ACTIVE TRAVEL		ALL STAFF, TRAINEES (R&W), SUPPLY (READ ONLY)
	ASSEMBLIES		
	ASSESSMENT FOR LEARNING		
	BEHAVIOUR MANAGEMENT		
	CPD	Any staff training materials including; Safeguarding, GDPR, Twilights etc.	
	CURRICULUM	All subject curriculum resources incl. Forest	

		Schools, MAC/RAC/WAC, topic webs, homework grids	
	FONTS – DO NOT DELETE		
	GOLDEN VALUES		
	ICT	Forms, guides, licence keys,	
	JOBSHEETS		
	LETTERS		
	NEWSLETTERS		
	PERFORMANCES		
	PLANNING	EYFS Planning, KS1 Planning, KS2 Planning	
	POLICIES		
	RESTORATIVE APPROACH		
	RISK ASSESSMENTS	All risk assessments except those pertaining to an Ed Visit.	
	SCHOOL ADMIN	Medical Forms, misc office documents, minutes template,	
	SCHOOL IMPROVEMENT	Raising attainment plans, Ofsted documents	
	SCHOOL PROJECTS	Children's Parade, Eco Schools, Fuel for School, Red Nose Day	
	SETTING UP A CLASSROOM		
	TIMETABLES		

	TRAINEE TEACHERS TRAINING PROGRAMME		
--	--	--	--

CHILDREN			ALL STAFF, TRAINEES (R&W), SUPPLY and PUPILS
	ASSEMBLIES		
	CLASSES		
	SINGING ASSEMBLY		