Wincheap Foundation Primary School

Cybersecurity Policy

Version	2
Ratified by	Finance & Premises Committee
Date of Approval	12th May 2026
Authors	Network Manager
Responsible Committee / Board	Finance & Premises Committee
Review Date	Spring 2027
Target Audience	Staff/Governors/Parents

Contents

Introduction

The Governors of Wincheap Foundation Primary School are committed to maintaining the confidentiality, integrity and availability of 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 includes the school's Cyber Response and Recovery Plan, and should be read alongside the Online Safety Policy and with reference to the following school policies:

- Data Protection Policy
- Disciplinary Policy and Procedure
- Behaviour Policy
- Clear Desk Clean Screen Policy
- Camera and Image Use Policy
- Acceptable Use Policy (AUP)

1. Legal framework

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

- Computer Misuse Act 1990
- General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Education Act 2002 (Safeguarding requirements)
- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children (2018, updated 2023)
- UK National Cyber Security Centre guidance
- Meeting Digital and Technology Standards in Schools and Colleges

2. Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within the school, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

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

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

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

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

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow

- Malicious breaches can occur as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data

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

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

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

3. Roles and responsibilities

The governing body 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.

The Headteacher will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Ensuring that a process exists whereby visitors that need access to the school system (e.g. Student Teachers) are identified to the Network Manager and receive appropriate induction in cyber security and online protection.
- 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 Computing Lead and Network Manager.
- 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.

The Network Manager will be responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Assessing the risks to the school in the event of a cyber-security breach.
- Working with the Headteacher after a data security breach to determine where weaknesses lie and improve security measures.
- Working with the Computing Lead to identify training needs for staff members on data security, network security and preventing breaches.
- Monitoring and reviewing the effectiveness of this policy, alongside the Headteacher, and communicating any changes to the Computing Lead/staff members.
- Maintaining an inventory of all IT hardware and software currently in use at the school.
- 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 and relevant guidance.
- Maintaining an up-to-date and secure inventory of all usernames and passwords.
- Removing any inactive users from the school system promptly and ensuring that this is always up-to-date.
- Performing a back-up of all electronic data held on the school server.
- 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.
- Leading on the school's response to incidents of data security breaches, including leading the cyber recovery team and liaising with third-party service providers and any other relevant organisations.

Note: With the agreement of the Headteacher, appropriate tasks above can be delegated to a third party security provider or within the network management team. Where any of these functions are subcontracted to third-party service providers, the Network Manager must have vetted them beforehand and will liaise and oversee the services they provide.

The Computing Lead will be responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within the school and promoting online safety measures to parents.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy.
- Working with the Network Manager to monitor online safety incidents which could result in data breaches and reporting these to the Headteacher.
- 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 Headteacher and Network Manager.

The Designated Safeguarding Leads (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:

- Accessing the school system, any communications received and websites on the internet with due regard to their responsibilities as outlined in this policy and the Online Safety policy.
- Ensure that any files or data that they have on their computer or in their One Drive cloud storage is kept securely and only shared in ways that comply with this policy.
- Undertaking appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them where appropriate.

4. Secure configuration

An inventory will be kept of all IT hardware and software currently in use at the school. The inventory will be stored by the Network Manager and will be audited on a regular 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 Network Manager before use.

All systems will be audited on a termly basis by the Network Manager to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, e.g. when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords from individual users. 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.

The school will work from the five security controls outlined by the National Cyber Security Centre. These are:

- **Firewalls** – Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure configuration** – The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The school will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach.

- **Access control** – The more people have access to data, the 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.

- **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.

The Network Manager will:

- Protect every device 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 as they can be useful in detecting 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.

All devices will be set up in a way that meets the standards described in the technical requirements.

The Network Manager will maintain a system for monitoring logs and documenting decisions made on inbound traffic.

5. Network security

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

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

Centralised firewall deployment

The school's firewall will be deployed 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.

As the school's firewall is managed by a third party, the firewall management service will be thoroughly investigated by the Network Manager 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.

If necessary, 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 Network Manager, taking into account the level of security currently provided and any incidents that have occurred.

The school will be aware that security standards may change over time with changing cyber threats and adapt accordingly.

The school will ensure that the security of every device on its network is reviewed regularly.

The Headteacher will agree with the Network Manager 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.

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

The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The Network Manager will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. The Network Manager will update malware protection on a termly basis to ensure it is up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

Filtering of websites, as detailed in the 'User privileges and passwords' section of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the ICT technician.

The school will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. The Network Manager will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

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 Network Manager will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

The school will use anti-malware software that:

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

7. User privileges and passwords

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

The Headteacher will clearly define what users have access to and will communicate this to the Network Manager. The Network Manager 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 breaches or attacks on the network.

All staff will be required to ensure they have a secure 'complex' password and change if they become known to other individuals, in line with the 'Secure configuration' section of this policy. Where appropriate, pupils are responsible for remembering their passwords; however, the Network Manager will be able to reset them if necessary. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible. The school does not currently use any form of biometric data or biometric security systems. Should such measures be introduced in the future, we will ensure that all relevant policies, procedures, and privacy notices are updated in full compliance with the Data Protection Act 2018 and UK GDPR.

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 'complex' in form and changed if there is a breach or shared with another user.

Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the school. The Network Manager will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

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

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

User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data.

Users will have a separate account for routine business if their main account:

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

The school will use multi-factor authentication as far as possible, particularly for accounts that have access to sensitive or personal data.

8. Monitoring usage

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

If a user accesses inappropriate content an alert is sent to the Headteacher.

The Headteacher will record any alerts using an incident log and will report this to the Network Manager or other staff members as appropriate. All incidents will be responded to in accordance with this policy, and as outlined in the Online Safety Policy.

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

All data gathered by monitoring usage will be kept on a secure shared drive for easy access when required. This data may be used as a method of evidence for supporting an as-yet undiscovered 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 and Cloud Storage controls

The school understands that some staff may need to access the school network from outside the school premises. If this is necessary, effective security management must be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The Network Manager will encrypt all school-owned devices for personal use, such as laptops and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Before distributing any school-owned devices, the Network Manager will ensure that manufacturers' default passwords have been changed.

When using laptops, tablets and other portable devices, the Headteacher will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the school premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any school-owned laptops, tablets or other devices, or when accessing school networks.

The Network Manager will ensure the use of encryption to filter the use of websites on school-owned devices in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises. The school uses tracking technology where possible to ensure that lost or stolen school-owned devices can be retrieved.

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.

Staff are provided with their own One Drive cloud storage service and should not use thumb drives/USB data sticks or similar removable storage methods to prevent the accidental access to, or leakage of, data. The sharing of files from a staff member's One Drive must only happen in line with the provisions in this policy and other relevant school policies.

The Wi-Fi network at the school will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless agreed prior to usage. A separate Wi-Fi network will be established for visitors at the school to limit their access to school networks and any other applications which it is not necessary for them to access.

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 training regarding what to do if a data protection issue arises from any home working or remote learning. This training must be reviewed annually by the Computing Lead and where necessary staff training should be refreshed.

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. Any data or files that are stored on a staff member's One Drive must be used in line with Section 9 above.

Staff and pupils may be required to use their own devices for the duration of a remote working or learning period. Using a shared personal or household device for school purposes should be avoided where possible; however, the school understands that this may not always be possible.

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

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 Network Manager, e.g. secure passwords and anti-virus software.

Staff will be informed that caution should be exercised while accessing personal data if a pupil or an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device must be locked.

Personal data should only be accessed on a home device if this is necessary for the member of staff to carry out their role. When working with 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 must be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

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

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

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the school premises to allow staff to work from home, it 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.

Pupils (and parents if the pupil has been allowed access to a school-owned device or software for use at home) are not permitted to use school-owned devices or software for activities that do not pertain to the child's online education, e.g. use of social media, gaming, streaming or viewing content that is not applicable to their curriculum. Pupils or parents are not permitted to download any software onto school devices, unless instructed to and approved by their teacher.

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

Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact the class teacher 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 Network Manager 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 Network Manager will provide staff and pupils with details and instructions for accessing the school network that they will be using throughout the duration of the remote working and learning period.

In the event that a staff member or pupil decides to leave the school permanently, all data in any form will be returned on or before their last day.

11. Backing up data

The server performs an automated backup every evening of all electronic data on the physical onsite server. Electronic data on user's One drive, Office 365 email, Sharepoint and on Teams is stored within Microsoft's Cloud. The Network Manager will ensure back-ups are running as normal, alongside a list of the files that have been included in the back-up.

The Network Manager will ensure that there are backup copies of important data, on at least two separate devices – one of which will remain off-site, e.g. cloud backups.

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

The school must 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 the Cloud to store backed-up data.
- Referring to the NCSC's Cloud Security Guidance.
- Ensuring that backing up data is regularly practised.

Where possible, 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 a secure remote server. Data will be replicated and stored in accordance with the school's Data Protection Policy. Only authorised personnel will be able to access back-ups of the school's data.

The school will ensure that offsite back-ups are secured.

The school's back-up strategy is automatically verified upon completion. These logs are kept for review if required.

12. Avoiding phishing attacks

The Network Manager 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.

Two-factor authentication must be used on any important accounts, such as the Headteacher's or School Business Manager's accounts.

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?
- Is the web address spelled correctly, corresponding to the name you would expect and without extra characters or grammar points in the name?

The Network Manager will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy. The Network Manager 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 unnecessary personal information, the Headteacher 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 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.

13. User training and awareness

The Network Manager should refer to the advice on the NCSC website or similar to help keep up to date with best practice. at https://www.ncsc.gov.uk/section/exercise-in-a-box/overview

The Computing Lead and Headteacher will arrange training for pupils and all staff who have access to the school system to ensure they are aware of how to use the network appropriately. 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 NCSC website has free training resources that might be useful for this. https://www.ncsc.gov.uk/blog-post/cyber-security-for-schools

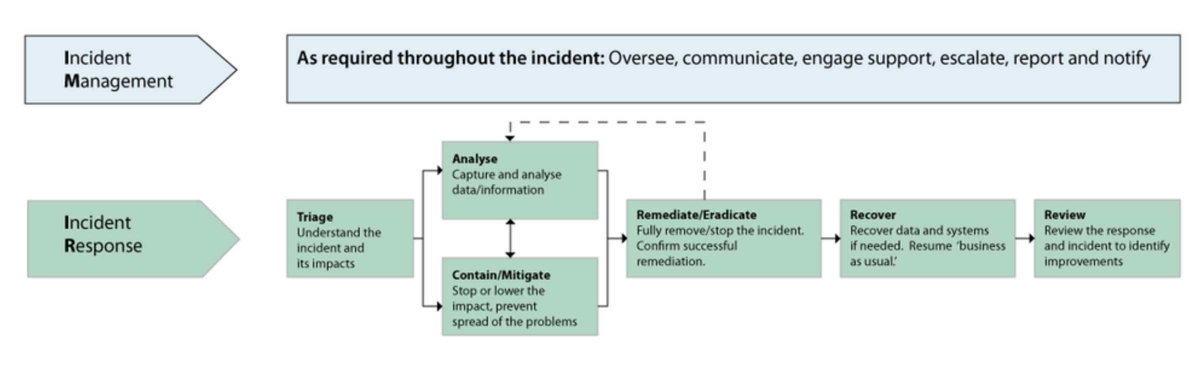
The Computing Lead will arrange for staff and pupils to undertake the appropriate training relating to online safety issues.

The Computing Lead and Headteacher will also arrange training for pupils and staff on a regular 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 Computing Lead and Headteacher within two weeks of 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. All staff will receive training as part of their induction programme. All pupils will receive training upon joining the school.

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 Discipline and Conduct Policy.

14. Incident Response and Recovery Plan



All cyber-security incidents will be managed in line with the school's Incident Response and Recovery Plan. In the event of the Headteacher being off-site, all actions in this plan will be carried out by her designated proxy. In the event of the Network Manager being off-site, the Headteacher will liaise with the IT technician. SNS, who provide the school's network security services, will act as third line support.

Triage

Any individual that discovers a cyber-security incident will report this immediately to the Headteacher and the Network Manager. They will decide who needs to be on the Cyber Recovery Team to investigate, contain and restore.

When an incident is raised, as part of the response the Network Manager will need to find out:

- Who reported it?
- What happened and when?
- What is the impact?
- What devices and systems are affected?
- Who can help investigate and respond?
- Does it affect individuals or organisations outside the school?

Action

The Network Manager will take the lead in investigating the incident, with assistance from the cyber recovery team, and will be allocated the appropriate time and resources to conduct this. The Network Manager, will as quickly as reasonably possible to contain the breach and restore network integrity. S/he will ascertain the severity of the incident and determine if any personal data or school system has been compromised.

Review

After the breach has been contained and the network integrity restored, the Network Manager will oversee a full investigation and produce a report which will include the information mentioned above.

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.

If the Network Manager 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
- Where appropriate, the Headteacher will deal with the pupil or member of staff who caused the breach in accordance with the Behavioural Policy or Discipline and Conduct Policy
- The school will work with the third-party service to provide an appropriate response to the attack, including any in-house changes
- The school will organise updated staff training following a breach within two weeks
- 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 Network Manager and Headteacher will establish what steps need to be taken to prevent further data loss, which may require support from various school departments and staff, and third party service providers. 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.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the Headteacher must inform the police of the security breach.

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 Headteacher and Network Manager decide 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.

The Headteacher 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.

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 Headteacher
- 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

The Headteacher will report a personal data breach via the ICO website. If the Headteacher is unsure whether a reportable breach has happened, s/he should make use of the ICO's self-assessment tool to determine whether reporting a breach is necessary.

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.

Where the school has been subject to online fraud, scams or extortion, the Headteacher will also report this using the Action Fraud website.

The Network Manager will test all systems to ensure they are functioning normally, and report the outcome to the Headteacher. 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

The following questions will be considered by the Network Manager to fully and effectively assess the risks that the cyber-security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the Network Manager's report, which should record:

- What type of, and how much, data is involved?
- How sensitive is the data? Sensitive data is defined in the UK 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 and/or 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?

In the event that the Network Manager 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 Headteacher and Network Manager 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 Headteacher and Network Manager 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. In line with the 'Data security breach incidents' section of this policy, if a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The Headteacher 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 Headteacher will consider, as necessary, the need to notify any third parties, such as the 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 Network Manager and Headteacher will identify any weak points in existing security measures and procedures, and will work to improve security procedures wherever required. The Computing Lead and Headteacher will identify any weak points in levels of security awareness and training and address these within two weeks of the breach.

The Headteacher will document all the facts regarding the breach, its effects and the remedial action taken and place these before the Governors. This should be an evaluation of what happened based on the Network Manager's report, what was done about it, and what actions need to be taken forward.

The Governors 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.

18. Monitoring and review

This plan will be reviewed by the Headteacher and the Network Manager on an annual basis. It will then be ratified by the Personnel and Pay Committee of the Governing Body.

The Network Manager and Computing Lead will be responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.