Full Governors
17.09.25
Signed .....

Cyber Security Policy

Portway Infant 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.

Legal framework

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

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- (DfE) (2025) 'Meeting digital and technology standards in schools and colleges

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,
- **Unauthorised removal of data** – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g., a staff member with authorised access who passes the data on to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.
- **Damage to physical systems** – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.
- **Unauthorised damage to data** – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

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

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

- Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision
- Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:
- The incorrect installation of antivirus software and/or use of outdated software can make the school software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g., unrestricted access to the school network, can allow unauthorised individuals to access the school system
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten

Roles and responsibilities

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 governor completes basic cyber security training.

The headteacher (who is also the Online Safety Officer in their role as DSL) will be responsible for:

- Ensuring all staff members 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 basic cyber security training for staff members in conjunction with the online safety officer, to be completed annually.
- 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 DPO will be responsible for:

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

The ICT technician will be responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- Ensuring any out-of-date software is removed from the school systems.
- 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.

The office manager will be responsible for:

- Monitoring online safety incidents which could result in data breaches and reporting these to the DPO.
- Liaising with relevant members of staff on online safety matters, e.g., the DPO and ICT technician.

The headteacher will also act as the digital lead and will therefore be responsible for:

- Identifying and evaluating the school's most significant cyber risks.
- Recording historical incidents to inform future mitigation strategies.
- Monitoring user behaviour to highlight risks that may compromise cyber security.
- Working in conjunction with ICT support to:
    - Establish a clear reporting and escalation process for cyber risks.
    - Integrate cyber risks into the school's risk register and business continuity plan, with regular testing.
    - Maintain all cyber security documentation in multiple secure formats (e.g., cloud storage, printed copies).
    - Develop and maintain a Cyber Response Plan that meets requirements of the Risk Protection Arrangement (RPA) cover or any other relevant insurance scheme.
    - Notify governors of material risks as part of routine strategic reporting.
- Working in conjunction with the DPO to:
    - Complete and maintain a Record of Processing Activities (ROPA) for all systems processing personal or sensitive data.
    - Assess staff access levels and permissions, and verify the adequacy of password policies.
    - Ensure email security is configured to mitigate risks from spoofed or imitation emails.

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.
- Ensuring all staff can access appropriate training and resources 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.
- Acting as the named point of contact within the school on all online safety issues.

All staff members will be responsible for:

- Understanding their responsibilities in regard to this policy.
- Undertaking the appropriate training annually.
- Ensuring they are aware of when new updates become available and how to safely install them.
- Reporting any known or suspected cyber incidents immediately.

Secure configuration

An inventory will be kept of all ICT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. The inventory will be stored in the school office and will be audited on a yearly basis to ensure it is up-to-date. Any changes to the ICT hardware will be documented using the inventory and will be authorised by the ICT technician before use.

All systems will be audited on a termly basis by the ICT technician to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory. Any software that is out-of-date or reaches

its 'end of life' will be removed from systems, e.g., when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords from individual users. Passwords will be changed on an annual basis to prevent access to facilities which could compromise network security. 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 will consider referring to the five security controls outlined in the National Cyber Security Centre's (NCSC's) 'Cyber Essentials'. These are:

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

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.

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 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 compromise

ill 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.

Malware prevention

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

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

Staff will follow procedures for filtering and monitoring to keep pupils safe as set out in the Online Safety Policy. The school's filtering provider will be:

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

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

Filtering of websites, 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 ICT technician will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

Staff are not allowed to download applications; this can only be done by the ICT technician following 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.

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.

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.

The headteacher will clearly define what users have access to and will communicate this to the ICT technician, ensuring that a written record is kept. The ICT technician will ensure that user accounts are set up to allow users access to the facilities required, in line with the headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

All 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. Only the ICT technician has access to this inventory. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible, and must be used for access to sensitive data.

Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the school. The ICT technician 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 implement a user account creation, approval and removal process which is part of the school joining and leaving protocols.

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

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

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

Monitoring usage
Monitoring user activity is important for the early detection of attacks and incidents. The ICT technician will record any alerts using an incident log and will report this to the headteacher/online safety officer who will report to the DPO as appropriate. The DPO will then inform the headteacher/online safety officer as appropriate. All incidents will be responded to in accordance with the 'Cyber security incidents' section of this policy, and as outlined in the Online Safety Policy.

The ICT technician will ensure that websites are filtered on a weekly basis for inappropriate and malicious content. Any member of staff that accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the Online safety 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 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.

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

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the school premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such

as in coffee shops, when using any school-owned laptops, tablets or other devices, or when accessing school networks.

The online safety officer will use encryption to filter the use of websites on school-owned devices in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises. 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.

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

Home working

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

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

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

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

Staff 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.

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.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked. School devices will automatically lock after one minute of inactivity to avoid an unauthorised person gaining access to the device. Where staff are using a personal device, they will be advised that a similar function should be implemented.

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

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

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

Staff need to be mindful with regards to the security of data taken off premises and safeguard it accordingly.

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

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

The ICT technician will provide staff 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 decides to leave the school permanently, all data in any form will be returned on or before their last day.

Backing up data

The ICT technician performs a test of all electronic data held by the school on a termly basis and is a continuous process. Each test is retained for three months before being deleted. The ICT technician performs an incremental back-up on a monthly basis of any data that has changed since the previous back-up. The ICT technician will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

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

The 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.

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.

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 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.

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.

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

Avoiding phishing attacks

The ICT 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.

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?

The ICT technician 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 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.

Any phishing emails received can be reported to Action Fraud at report@phishing.go.uk.

User training and awareness

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

The headteacher will also arrange training for pupils and staff 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.

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

Staff with access to the school's IT network will be required to undertake basic cyber-security training upon induction which is refreshed every year. 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

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.

Cyber-security incidents

All cyber-security incidents will be managed in line with the school's Cyber Response Plan. **Appendix 1**

Any individual that discovers a cyber-security incident will report this immediately to the office manager or headteacher.

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

The school's DPO 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 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. 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.

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 member of staff who caused the breach, in accordance with the Behavioural Policy or Disciplinary Policy and Procedure
- The school will organise updated staff training following a breach
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

Where the security risk is high, the 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.

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.

Schools are required to report personal data breaches to the ICO if there is a likelihood of risk to people's rights and freedoms. These incidents must also be reported to the DfE sector cyber team and sector.incidentreporting@education.go.uk. 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.

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.

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 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 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.

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 DPO will also report this using the Action Fraud website.

Where the incident causes long term school closure or serious financial damage the DPO or Headteacher will also report the incident to the National Cyber Security Centre.

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.

Assessment of risks

The following questions will be considered by the DPO 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 DPO'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 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:
    1. Physical safety
    2. Emotional wellbeing
    3. Reputation
    4. Finances
    5. Identity
    6. 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?

Cyber risk is continually reviewed actions taken in line with new guidance or risk. These reviews are used to:

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

In the event that the DPO, 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.

Consideration of further notification

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 data security.

The DPO 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 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.
- 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 DPO 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.

Evaluation

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.

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.

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.

The DPO will report on findings and implement the recommendations of the report after analysis and discussion.

Reviewed autumn 2025
To be reviewed autumn 2026

Appendix 1

Cyber Incident Response Plan

Contents

Introduction
Portway Infant School IT Incident Management Plan has been developed to provide direction and focus to the handling of information security incidents that adversely affect the school. This plan applies to any person or entity charged by the headteacher with a response to information security related incidents at the school.

The purpose of this document is to allow Portway Infant School to respond quickly and appropriately to information security incidents.

Event Definition
Any observable occurrence in system, network, environment, process, workflow, or personnel. Events may not be negative in nature.

Adverse Events Definition
Events with a negative consequence, this plan only applies to adverse events that are computer security related, and not those caused by natural disaster, power failures etc.

Incident Definition
A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardises the confidentiality, integrity, or availability of information resources or operations. A security incident may have one or more of the following characteristics:

- Violation of an explicit or implied security policy
- Attempts to gain unauthorised access to an Information Resource
- Denial of service to an Information Resource
- Unauthorised use of Information Resources
- Unauthorised modification of information
- Loss of Confidential or Protected information

Roles & Responsibilities

Role	Responsible Person	Contact Information	Escalation (1- 3)*
Incident Response Leader	Headteacher	head@portwayi.derby.sch.uk	1
Deputy Incident Response Leader	Office Manager	admin@portwayi.derby.sch.uk	1
Technical Lead	IT Support	administrator@portwayi.derby.sch.uk	1
Local Incident Advisor	Headteacher	head@portwayi.derby.sch.uk	3
On Site Technician	IT Support	administrator@portwayi.derby.sch.uk	3

*Escalation level determines order in which notification should occur:
Notify first, required on all incidents (1, 2, 3)
Required on all moderate or high-severity incidents Involve
as needed (3)

Cyber Security Incident Handling Team (IHT)
- Consists of SLT, IT Leadership, and Data Protection Officer.
- Advise on incident response activities relevant to their area of expertise.
- Maintain a general understanding of the Plan and policies of the organisation.
- Ensure incident response activities are in accordance with legal, contractual, and

regulatory requirements.

- Participate in tests of the incident response plan and procedures.
- Responsible for internal and external communications pertaining to cyber security incidents.

Cyber Security Incident Response Team (CSIRT)

The CSIRT is comprised of SLT, IT Lead & School management and co-opted experienced personnel. The role of the CSIRT is to promptly handle an incident so that containment, investigation and recovery can occur quickly. Where third-party services are leveraged, ensure they are engaged as necessary. Roles within the CSIRT include:

- **IT Service Lead**

The Tech Support Manager, or in their absence a nominated individual by the IHT takes the role of the incident response managers – and oversees and prioritises actions during the detection, analysis, and containment of an incident. They are also responsible for conveying the special requirements of high severity incidents to the rest of the organization as well as communicating potential impact to the governors. Additionally, they are responsible for understanding the SLAs in place with third parties, and the role third parties may play in specific response scenarios.

- Coordinate response activities within the school and external resources as needed to minimise damages to information resources.
- Provide updates on response activities to the SLT.
- Ensure service level agreements with service providers clearly define expectations of the organisation and the service provider in relation to incident response.
- Review the Cyber Security Incident Response Plan ("the Plan") to ensure that it meets policy objectives and accurately reflects the goals of the school. Seek Plan approval from the headteacher.
- Approve close of moderate or critical-severity incidents.
- Ensure lessons learned are applied/weighed based on risk for Severity 1 incidents.

Further responsibilities:

- Act as a liaison for all communications to and from the Information Governance Officer (IGO).
- Assemble a Cyber Security Incident Response Team (CSIRT).
- Ensure personnel tasked with incident response responsibilities are trained and knowledgeable on how to respond to incidents.
- Update Plan and procedures as needed based on results from testing, incident response lessons learned, industry developments and best practice.
- Review the Plan and procedures at least annually.
- Initiate tests of the Plan and procedures at least annually.
- Ensure team activities comply with legal and industry requirements for incident response procedures.
- Act as the primary Incident Response Manager, responsible for declaring a cyber security incident, managing team response activities, and approving close of Severity2 & 3 incidents

- **Incident Response Team Members**

The Incident Response Manager is supported by technical staff that work directly with the affected information systems to research the time, location, and details of an incident.

Further responsibilities:

- Assist in incident response as requested. CSIRT responsibilities should take priority over normal duties.
- Understand incident response plan and procedures to appropriately respond to an incident.
- Continue to develop skills for incident response management.
- Ensure tools are properly configured and managed to alert on security incidents/events.
- Analyse network traffic for signs of denial of service, distributed denial of service, or other external attacks.
- Review log files of critical systems for unusual activity.
- Monitor business applications and services for signs of attack.
- Collect pertinent information regarding incidents at the request of the IRCommander.
- Consult with qualified information security staff for advice when needed.
- Ensure evidence gathering, chain of custody and preservation is appropriate.
- Participate in tests of the incident response plan and procedures.
- Be knowledgeable of service level agreements with service providers in relation to incident response.

Incident Response Framework

The school recognises that, despite reasonable and competent efforts to protect Information resources, a breach or other loss of information is possible. The school must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to staff, students, parents, customers, partners, and the organisation itself.

The incident response framework is comprised of six phases that ensure a consistent and systematic approach.

Phase I – Preparation

It is essential to establish a **C**yber **S**ecurity **I**ncident **R**esponse **T**eam (CSIRT), to define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools.

The members of the **CSIRT** should meet regularly throughout the year. During the meeting, the **CSIRT** should be presented with an overview of the MATs currently risk analysis and any works required or have taken place that may affect (negatively or positively) the readiness of the MAT systems.

Incident Type	Reporting Method	Available To
Website defacement, data modification or exposure	Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)
Impact on IT Support functionality	Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)
Impact on T&L	Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)
Impact on business continuity	Social Media Text message and Email alerts Paper comms	Internal and external (to be decided by CSIRT)

Phase II – Identification and Assessment

Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements.

Events versus Incidents

Events are observed changes in normal behaviour of the system, environment, process, workflow, or personnel. Incidents are events that indicate a possible compromise of security or non-compliance with policy that negatively impacts (or may negatively impact) the organisation.

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security incidents, which may include any or all the following:

- email or phone notification from an intrusion detection tool;
- suspicious entries in system or network accounting, or logs;
- discrepancies between logs;
- repetitive unsuccessful logon attempts within a short time interval;
- unexplained new user accounts;
- unexplained new files or unfamiliar file names;
- unexplained modifications to file lengths and/or dates, especially in system files;
- unexplained attempts to write to system files or changes in system files;
- unexplained modification or deletion of data;
- denial/disruption of service or inability of one or more users to login to an account;
- system crashes;
- poor system performance of dedicated servers;
- operation of a program or sniffer device used to capture network traffic;

- unusual time of usage (e.g. users login during unusual times);
- unusual system resource consumption (High CPU usage);
- last logon (or usage) for a user account does not correspond to the actual last time the user used the account;
- unusual usage patterns (e.g., a user account associated with a user in finance is being used to login to an HR database);
- unauthorised changes to user permission or access.

Note: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information or evidence required for a forensic investigation later. **Only power off the system if it cannot be disconnected from the wired and wireless networks completely.**

Reporting an Event or Incident

On the discovery of a potential event – the discover of the issue (or the IT Support team member who has actioned a query which has identified an event) must immediately make the ULT IT Service Lead aware of the discovered incident. The Information Governance Officer (IGO) should also consider if the incident should be reported to Information Commissioners Office (ico).

Incident Scope

Determining the scope will help the IT Service Lead understand the potential business impact of the incident. The following are some of the factors to consider when determining the scope:

- How many systems are affected by this incident?
- Is Confidential or Protected information involved?
- what is/was the entry point for the incident (e.g., Internet, network, physical)?
- What is the potential damage caused by the incident?
- What is the estimated time to recover from the incident?
- What resources are required to manage the situation?
- How could the assessment be performed most effectively?

Incident Impact

Once the categorisation and scope of an incident has been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken to provide a resolution; however, in all instances an incident report must be completed and reviewed by the Incident Response Commander.

Functional and informational impacts are defined with initial response activity below:

Functional Impact	Definition	CSIRT Response
None	No effect to the organisation's ability to provide all services to all users.	Create ticket and assign for remediation.
Limited	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.	Create ticket and assign for remediation, notify the IGO and IHT.
Moderate	The organisation has lost the ability to provide a critical service to a subset of system users.	Initiate full CSIRT, involve the IGO and IHT
Critical	The organisation is no longer able to provide some critical services to any user.	Initiate full CSIRT, IGO, and IHT. Consider activation of the Disaster Recovery Plan

Once a potential incident has been identified, part or all of the CSIRT will be activated by the IT Service Lead to investigate the situation. The assessment will determine the category, scope, and potential impact of the incident. The CSIRT should work quickly to analyse and validate each incident, following the process outlined below, and documenting each step taken.

Information impact	Definition	CSIRT Response
None	No information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	No action required
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the data owners to determine the appropriate course of action.
Moderate	Internal Information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the IGO and IHT. IGO will work with management, legal, and data owners to determine appropriate course of action.

Critical	Protected Data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the IGO and IHT. IGO will work with legal to determine whether reportable, and the appropriate notification requirements.

The Incident Handling Log & Assessment Tool and Response Level table below will help determine the severity of the incident and urgency of response activities.

Response Level Classification		**Informational Impact**			
		None	**Limited**	**Moderate**	**Critical**
Functional Impact	**None**	N/A	P. 3	P. 2	P. 1
	Limited	P. 3	P. 3	P. 2	P. 1
	Moderate	P. 2	P. 2	P. 2	P. 1
	Critical	P. 1	P. 1	P. 1	P. 1

Phase III – Containment and Intelligence

Containment of the incident is necessary to minimise and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties.

Containment Strategies

Use the list of strategies below to choose the procedure(s) most appropriate for the situation.

- stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks;
- ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed;
- if DOS/DDOS - control WAN/ISP;
- virus outbreak – contain LAN/system;
- data loss – review user activity, implement data breach response procedures;
- website defacement – repair site, harden from future attacks;
- compromised API – review changes made, repair API, harden from future attacks.

Common Containment Steps
Containment requires critical decision-making related to the nature of the incident. The IT Service Lead and other members of SLT should review all the containment steps listed below to formulate a strategy to contain and limit damages resulting from the incident.

All attempts to contain the threat must consider every effort to minimise the impact on the business operations. Third-party resources or interested parties may need to be notified. Where law enforcement may become involved, efforts must be made to preserve the integrity of relevant forensic or log data and maintain a clear chain-of-custody. Where evidence cannot be properly maintained due to containment efforts, the introduced discrepancy must be documented.

When evaluating containment steps, consider the following:

- Enable disposable administrative accounts for use during the investigation and reset associated passwords if believed to have been at risk of compromise while in being used.
- Will the ability to provide critical services be impacted? How? For how long?
- Is a legal investigation or other action likely? Does evidence need to be preserved?
- How likely is the containment step to succeed? What is the result, full containment or partial?
- What resources are required to support the containment activity?
- What is the potential damage to equipment and other resources?
- What is the expected duration of the solution? (Temporary, short-term, long-term, or permanent)
- Should IR team members act discreetly to attempt to hide their activities from the attacker?
- Is the assistance of a third party required? What is the expected response time?
- Do interested parties (parents, staff, students, clients) need to be notified? If so, when?
- Does the impact to equipment, network, or facilities necessitate the activation of the Disaster Recovery Plan?

Engage Resources
The CSIRT should select the option based on the severity of the incident, the damage incurred and legal considerations.

	In-house investigation	Law enforcement	Private forensic specialist
Time Response	Quick response	Varies by area and agency	Quick response
Competency	Skills vary	Depends on local law enforcement	Highly skilled, often with law enforcement background
Preservation of evidence	Does not ensure evidence integrity	Preserve evidence integrity and present evidence in court	Preserve evidence integrity and present evidence in court
Reputation impact	Minimal effect	Potential loss of reputation if certain incidents reach public	Potential loss of reputation if certain incidents reach public

Reduce Impact

Depending on the type of incident, the team must act quickly to reduce the impact to affected systems and/or reduce the reach of the attacker. Actions may include, but are not limited to the following:

- stop the attacker using access controls (disabling accounts, resetting active connections, changing passwords, implementing router ACLs or firewall rules, etc.);
- isolate compromised systems from the network;
- avoid changing volatile state data or system state data early on;
- identify critical external systems that must remain operational (e.g., email, client application, DNS) and deny all other activity;
- maintain a low profile, if possible, to avoid alerting an attacker that you are aware of their presence or giving them an opportunity to learn the CSIRT's tactics, techniques, or procedures;
- to the extent possible, consider preservation of system state for further investigation or use as evidence.

Collect Data and Increase Activity Logging

Increase monitoring and packet capture on affected systems while the CSIRT investigates the scope and impact of the incident. Continue increased logging and monitoring as you move onto the Eradication and Recovery phases.

- enable full packet capture;
- collect and review system, network, and other relevant logs;
- create a memory image of impacted systems;
- take a forensic image of affected systems;
- monitor possible attacker communication channels.

Conduct Research
Performing an Internet search, consulting third party resources, and/or consulting IT using the apparent symptoms and other information related to the incident you are experiencing may lead to more information on the attack.

Notify Interested Parties
Once an incident has been identified, determine if there are others who need to be notified, both internal (School Leadership etc.) and external (e.g., service providers, government, public affairs, media relations, parents and students, staff, general public, etc.). Always follow the "need to know" principle in all communications. Most importantly, remain factual and avoid speculation.

Depending on the degree of sensitivity of the incident, it may be necessary for Legal/Management to require employees to sign NDAs or issue gag orders to employees who need to be involved.

Investigation
As the CSIRT works to contain, eradicate, and recover from the incident, the investigation will be ongoing. As the investigation proceeds, you may find that the incident is not fully contained, eradicated, or recovered. If that is the situation, additional it may be necessary to revisit earlier phases (see Figure 1: PICERL Framework Model). The Containment, Eradication, and Recovery phases are frequently cyclical.

Phase IV – Eradication
Eradication requires removal or addressing of all components and symptoms of the incident. Further, validation must be performed to ensure the incident does not reoccur.

Steps to eradicate components of the incident may include:

- disable breached user accounts;
- reset any active sessions for breached accounts;
- identify and mitigate vulnerabilities leveraged by the attacker;
- close unnecessary open ports;
- increase authentication security measures (implement MFA, add geolocation restrictions);
- increase security logging, alerting, and monitoring;
- clean installation of affected operating systems and applications.

All re-installed operating systems and applications must be installed according to system build standards, including but not limited to:

- applying all the latest security patches;
- disabling all unnecessary services;
- installing anti-virus software;
- applying hardened system configuration baselines;
- changing all account passwords (including domain, user and service accounts).

NOTE: It may be possible to restore the system without the need to perform a full clean installation. IT personnel, at the direction of the CSIRT, will make this determination.

Phase V – Recovery

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned.

Prior to restoring systems to normal operation, it is critical that the CSIRT validates the system(s) to determine that eradication was successful, and the network is secure. Once the organisation has been attacked successfully, the same attackers will often attack again using the same tools and techniques leveraged in the initial attack. Having gained access to the compromised system(s) or network once, the attacker has more information at their disposal to leverage in future attacks.

If feasible, the system should be installed in a test environment to determine functionality prior to reintroduction into a production environment.

Furthermore, network monitoring should be implemented for as long as necessary to detect any unauthorised access attempts.

Recovery steps may include:

- restoring systems from a clean backup;
- replacing corrupted data from a clean backup;
- restoring network connections and access rules;
- communicating with interested parties about changes related to increased security;
- increasing network and system monitoring activities (short or long-term);
- increasing internal communication/reporting related to monitoring;
- engaging a third party for support in detecting or preventing future attacks.

Phase VI – Lessons Learned

The Lessons Learned phase includes post-incident analysis on the system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned from the incident are communicated to the SLT and governors and action plans developed to improve future incident management practices and reduce risk exposure.

Russell Eales
IT Support
Reviewed autumn 2025
To be reviewed autumn 2026