PENAIR SCHOOL

DISCE UT VIVAS

IT Services Information Security Policy

Policy holder:	Business Manager
To be reviewed by policy holder:	Annually
Last reviewed by policy holder:	Summer 2026
Next review by policy holder:	Summer 2027
Reviewed by Board at:	Business, Audit & Risk Committee
Date approved by Board:	Summer 2026
Next review by Board:	Summer 2027
Version:	2

1 Introduction 3
2 Applicability & Scope 3
3 Policy Statement 3
4 Risk Assessment 4
5 Business Continuity 4
6 Physical and environmental security 4
7 Security of Information Systems 4
8 Asset Classification and control 5
9 Requirements for retention and disposal of information 5
10 Information Security Awareness 5
11 Enforcement 6
12 Responsibilities 6
13 Appendices 8

1 Introduction

Information and information systems are valuable assets. Through policies, procedures and structures Penair School (Penair / the School) strives to secure an uninterrupted flow of information, internally and externally. The School believes that information security is essential to ensure effective data sharing, and to support its academic and business objectives. The following principle will be applied in the design and management of Information Security:

Data, whether stored, in transit, or in use, is to be protected from unauthorised use and disclosure, thereby ensuring that confidentiality, integrity and accessibility are maintained.

2 Applicability & Scope

This policy applies to all Information and Information Systems owned by the School, including information and systems maintained by third parties on behalf of the Trust.

3 Policy Statement

Information is an essential asset that needs to be protected, especially in an increasingly interconnected communications environment. Information security measures protect information from a wide range of threats and safeguard based on the following security principles:

1. **Confidentiality** - through protection from unauthorised access and disclosure.
2. **Integrity** - by ensuring the accuracy and completeness of information and of processing methods.
3. **Availability** - by ensuring that information and associated services are available to authorised users when required. Information exists in many forms and includes printed material and electronic data, video, audio and text content.
4. **Accountability** - by tracing actions and events back in time to the users, systems, and processes that performed them, to establish responsibility for actions or omissions.

Whatever form information takes and however it is shared or stored, all School information will be appropriately protected.

Lawful and appropriate management of systems and data is not only a corporate responsibility but a personal one. Users will be held individually accountable for their own actions.

With reference to the Laws and regulations in the References section the school will strive to ensure that:

- Systems and information comply with and are used within the framework of the law (including those listed in the external references section). This includes regulating access and monitoring communications.
- Information content remains lawful. This includes checking data and software across all School IT services.

- Special care will be exercised in managing personal and commercially confidential data.

This Policy is brought to the attention of all new members of staff and affiliates. It is the responsibility of existing staff and all other users including contractors to routinely check the status of this Policy for updates and revisions, and other relevant School rules.

4 Risk Assessment

Full risk assessments will be performed annually across the School to address the vulnerabilities of information content and system and current threats. The School Board of Governors review the effectiveness of risk management processes on behalf of the Board of Governors.

The Head Teacher and other senior staff within schools are responsible for ensuring effective risk management in their own areas.

5 Business Continuity

Information security forms part of wider business continuity planning within the School. Information security requirements will be regularly and routinely reviewed and assessed accordingly.

6 Physical and environmental security

Appropriate security measure will be installed and enforced to prevent unauthorised access, damage and interference with information and facilities.

To prevent loss, damage or compromise of assets and disruption of business activities, information and equipment will be protected as far as possible from environmental hazards both natural and manmade. This includes reasonable protection against power failures and the establishment and maintenance of an offsite alternative operating centre where justified and achievable.

7 Security of Information Systems

Rules for accessing Schools' information facilities, the responsibilities of users and the rights of the School are set out in the Acceptable Use policy which all staff and pupils are required to comply with.

The following security measures are supported by the School to ensure the security of information and information systems:

- Strong identity management for users and information systems.
- Proper authorisation and access control for users and information systems.
- 2 factor authentication when accessing the school network outside of school
- Appropriate encryption for information and subsequently the data in motion and at rest.
- Information and system backup and recovery.

- Regular audit to ensure that only licensed and authorised software is used across IT within the School.
- Appropriate protection against malicious software and other forms of attack against IT in the School.
- Users should recognise that inappropriate software interferes with the proper running of Penair systems and should not be installed or used.
- Any authorised software should be used only within the terms of its licence and should be properly maintained and upgraded.
- School information must remain secure when it is taken of viewed away from School premises. Responsibility of data housed on mobile devices (phones, tablets, laptops, USB devices, digital storage devices and so on) rests with the user in control of the devices. Users should take appropriate measures to secure both the data and the devices. USB storage devices must be encrypted and password protected.
- The requirement for security of information outside the School applies equally to paper records and files.

8 Asset Classification and control

To ensure effective asset protection the School will develop and maintain asset registers of hardware, software and information. All information and systems should be labelled with relevant information classification

The following working practices should be implemented and monitored at a department level:

1. Never leave sensitive or confidential documents unattended, or easily accessible.
2. Secure storage, including lockable filing cabinets and password protected computer files.
3. A nominated security officer to maintain access lists and administer permissions.
4. Careful consideration about the best and most secure medium for communication and retention of secure information.

9 Requirements for retention and disposal of information

Retention and disposal rules are addressed in the Data Protection Policy (see disposal of records section) which is available on the school website here Penair School Data Protection Policy .

Confidential and sensitive material must always be disposed of securely; physical records must be shredded or incinerated, digital data should be securely erased under advice from the IT Manager.

10 Information Security Awareness

Information security awareness is vital and the School will make efforts to ensure that users of information systems are informed and updates about best practices and current risks. All users of School information and information services (including contractors) will receive appropriate information about the security standards.

Data protection training is available to all staff through SchoolPro.

11 Enforcement

Any registered user found to have violated this policy will be in breach of School regulations. Breaches will be subject to disciplinary procedures as deemed appropriate.

12 Responsibilities

Role	Responsibility
Users of Penair IT Systems, information systems and networks.	Members of the School using School information systems and networks will act lawfully and responsibly and in full compliance with all relevant policies and procedures when handling and sharing School data, in whatever format (i.e. digital or physical). Third parties who manage, process, transmit or store information, or information system on behalf of the School will act responsibly and in full compliance with this Policy and all relevant policies and procedures when handling and sharing School data.
IT Manager	Responsible for: • Administering access to School's Active Directory environment and many of its systems • Hardening end user systems • Implementing role based access control upon the School's shared access file systems • Creating the School's Active Directory user accounts, maintaining network infrastructure, firewalls and network zoning

Governance	The School's Leadership Team supported by the IT Manager ensures that security is properly evaluated and managed across the School. IT Governance is responsible for: • Writing and maintaining this policy • Investigating security incidents and breaches and recommending remedial actions • Assessing information and security risks. • Identifying and implementing controls to risks.

Related Documents

PCI DSS Standard v4.0.1	https://www.pcisecuritystandards.org/document_library
The Computer Misuse Act 1990	https://www.legislation.gov.uk/ukpga/1990/18/contents
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000	The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Data Protection Act 1998	https://www.legislation.gov.uk/ukpga/1998/29/contents
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)	General Data Protection Regulation (GDPR) – Legal Text
The Copyright Designs and Patents Act 1988	https://www.legislation.gov.uk/ukpga/1988/48/contents

13 Appendices

Password Policy for Users – Appendix 1

This policy defines the standards for creating, using, and managing passwords to protect the school's systems, data, and users from unauthorised access.

1. Scope
This policy applies to all staff, students, governors, contractors, and visitors with access to school IT systems.

2. Password Creation Requirements
Passwords must be at least 12 characters for staff and 8 characters for students and include three of the following: uppercase letter, lowercase letter, number, special character. They must not contain names, school names, or common predictable patterns.

3. Password Management Requirements
Passwords must be changed annually or immediately if compromise is suspected. Reuse of the last three passwords is not permitted.

4. Multi-Factor Authentication (MFA)
MFA must be enabled where available, especially for staff and administrative accounts.

5. Responsibility of Users
Users must keep passwords confidential, never share them, and report suspected compromise immediately.

6. Password Storage
Passwords must not be stored in plain text, emails, or written visibly. Secure password managers may be used.

7. Student Password Requirements
Students Passwords must be a minimum of 8 characters and contain 3 of the 4 following requirements. Upper case letters, Lower case letters, Numbers, or special characters.

8. Administrative & Privileged Accounts
Administrator accounts must use passwords with 15+ characters, MFA, and separate daily-use accounts.

9. Enforcement
Non-compliance may result in forced resets, suspension, or disciplinary action.

10. Review Cycle
This policy is reviewed annually or after cybersecurity incidents.

Student Acceptable Use Policy – Appendix 2

Penair School – ICT Acceptable Use Policy (Student)

Why we have this policy

Technology is an important part of learning at Penair School. We want to help you use the internet and digital devices safely, responsibly, and confidently. This agreement explains what is expected when you use school computers, your own devices, or the internet for anything related to school.

Staying Safe Online

- The school can monitor how I use the computers, internet, email, and other digital tools.
- I will keep my username and password private and never use someone else's login.
- I will be careful when talking to people online and understand that not everyone is who they say they are.
- I will not share personal information about myself or others (like full name, address, phone number, school details) on public websites or with strangers.
- I will not arrange to meet anyone I've only spoken to online. If something like that ever happens, I will tell a trusted adult immediately.
- I will report anything online that seems worrying, inappropriate, or makes me feel uncomfortable.
- I understand that what I post online can affect others. I will not use the internet to insult, bully, or embarrass anyone.

Using Technology Responsibly

- School ICT systems are intended for learning. I won't use them for gaming, gambling, online shopping, or video streaming unless a teacher gives permission.
- I won't download or upload large files unless I have permission.
- I will communicate respectfully and politely in messages, emails, and online platforms.
- I will respect other people's work and will not try to access, change, or delete anyone else's files.
- I will not take or share photos or videos of anyone without their permission.
- I will not use my own devices on school grounds unless it is for essential medical reasons.

Using the Internet Properly

- If I use images, music, or information created by someone else, I will make sure I have permission.
- I won't download illegal or copyrighted materials.
- I know that not everything online is true, so I will think carefully and check information from more than one source.

Protecting School Equipment and Systems

- I will not try to access or download anything that could harm the school network or devices.
- I won't try to get around the school's security systems or filters.

- I will only use my own phone or device in school when I have permission.
- I understand that I am responsible for my own device if I bring it to school.
- I will report any damage or problems with ICT equipment as soon as I notice it.
- I will not open suspicious email attachments.
- I won't install software or change device settings on school computers.

My Behaviour Inside and Outside School

- I understand that this agreement still applies when I'm not at school if my behaviour affects members of the school community—for example, cyberbullying or sharing inappropriate content.
- I understand that breaking these rules may lead to consequences such as losing ICT access, my parents being contacted, or more serious actions if necessary.

Student Acceptable Use Agreement

By signing, I confirm that I understand and agree to follow all the rules in this policy when:

- I use school ICT equipment or logins (in school or at home)
- I bring my own devices to school (like a phone, tablet, or camera)
- I use my own devices at home for school-related activities

I understand that breaking these rules may lead to my ICT access being removed and other appropriate actions.

Name of Pupil:……..

Tutor Group: …….

Signed:…….(pupil)

Signed:…….(parent)

Signed:…….(tutor)

Date:…….

Adding signatures above cover all of the policies and agreements of Penair School which can be located on the Penair School website or on request.

Penair School – ICT Acceptable Use Policy (Staff) – Appendix 3

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policies on data protection, online safety, and safeguarding.
- Preventing disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our Staff Disciplinary Policy.

2. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Online gambling, inappropriate advertising, phishing, and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral.
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts, or data.
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to the school's ICT facilities
- Removing, deleting, or disposing of the school's ICT equipment, systems, programs, or information without permission from authorised personnel
- Causing data breach by accessing, modifying, or sharing data (including personal data) to which authorised personnel do not permit a user to have access, or without authorisation.
- Using inappropriate or offensive language
- Promoting a private business, unless that business is related to the school.
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic, or discriminatory in any other way.
- Using AI or AI tools in any way which breaches the Acceptable Use Policy

3. Exceptions from Unacceptable Use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

3.1 Sanctions

Staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies.

4. Use of School Supplied Equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations.
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g., when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device.
- Lock devices with a password when unattended. Passwords must:
- Not be shared with others and must be changed regularly
- Be suitably strong, in accordance with the school's password policy
- Not be reused across multiple accounts
- Update software, operating systems and applications when prompted, or as directed by the IT Support Team
- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks.
- Report any loss, theft, damage, or compromise of a school device promptly to the IT Support Team, designated safeguarding lead, and data protection officer.

4.1 Use of Phones and Email

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff must make sure multi-factor authentication is enabled on their email account(s). All work-related business should be conducted using the email address the school has provided. Staff must not share their personal email addresses with parents/carers and pupils and must not send any work-related materials using their personal email account.

Email messages are required to be disclosed in legal proceedings or in response to subject access requests from individuals under the UK GDPR and the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
Staff must take extra care when sending sensitive or confidential information by email.
If staff send an email in error that contains the personal information of another person, they must inform the IT Support Team immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the phones provided by the school to conduct all work-related business. School phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 2.

4.2 Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Head Teacher may withdraw or restrict this permission at any time and at their discretion.
Personal use is permitted provided that such use:

- Does not take place during Teaching Hours
- Does not constitute 'unacceptable use', as defined in section 2
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them. Staff should take care to follow the school's guidelines on use of social media and use of email to protect themselves online and avoid compromising their professional integrity.

4.3. Monitoring and Filtering of the School Network and Use of ICT Facilities

To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and to safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes:

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.

The school monitors ICT use to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures, and standards.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place.
- Staff are aware of those systems and trained in their related roles and responsibilities.
- It regularly reviews the effectiveness of the school's monitoring and filtering systems.

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place. Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

Penair School – Acceptable User Policy for iPads – Appendix 4

Introduction

The policies, procedures and information within this document applies to all iPads for use within the PE Faculty.

User Responsibilities

- Users must use a PIN code (Issued by IT Support)
- Users must use the provided protective covers/cases for their iPad.
- The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop or place heavy objects (books, laptops, etc.) on top of the iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without that person's consent.
- The iPad is subject to routine monitoring by IT Support).
- Devices must be surrendered immediately upon request by any member of the Senior Leadership Team.
- Users in breach of the Penair Acceptable Use Policy may be subject to but not limited to disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
- Personal files must not be created on the school iPad and Penair School is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.
- If the iPad is taken away from the school you will not be able to connect it to any other network (locked to Penair WiFi).
- All content should be treated as private and confidential.
- The iPad must not be used for any personal social media and networking purposes. However, photographs taken on the school iPad may be used for the school's marketing and social media purposes. Photographs and videos can also be taken for analysis of performance as part modelling and assessment in lessons.

Additional Responsibilities for Pupils

- Pupils must only use iPads with the permission of the teacher and their knowledge and whilst fully supervised.
- Pupils must follow the Acceptable User Policy when using the iPads.
- Pupils in breach of the Acceptable User Policy may be subject to but not limited to, disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Additional Safeguarding and Maintaining as an Academic Tool

- iPad batteries are required to be charged and be ready to use in school.
- Syncing the iPad to iTunes or iCloud will be maintained by a School IT administrator.
- Items deleted from the iPad cannot be recovered.
- Memory space is limited.
- The whereabouts of the iPad should be always known.
- It is a user's responsibility to keep their iPad safe and secure.
- iPads belonging to other users are not to be tampered with in any manner.
- If an iPad is found unattended, it should be given to the nearest member of staff.

Lost, Damaged or Stolen iPad – Staff

- iPad batteries are required to be charged and be ready to use in school.
- iPads must be password protected for secure access for the user only.
- Passwords must not be disclosed to any unauthorized people.
- If the iPad is lost, stolen, or damaged, the ICT Technicians/Network Manager/Head Teacher must be notified immediately.

Lost Prohibited Uses (not exclusive)

- Accessing Inappropriate Materials – All material on the iPad must adhere to the Penair ICT Acceptable Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Violating Copyrights – Users are not allowed to have music and install apps on their iPad.
- Cameras – Use of the camera and microphone is prohibited unless permission is granted by a teacher.
- Users must use good judgment when using the camera and that it is for educational purposes only. The user agrees that the camera will not be used to take inappropriate, illicit, or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. **Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation**.
- Images of other people may only be made with the permission of those in the photograph.
- Posting images/movies on the Internet into a public forum is strictly forbidden, unless the photographs are used in official Penair school digital marketing with the permission of all students involved.
- Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.
- Users should be aware of and abide by the guidelines set out by Penair School's Acceptable User Policy

- Penair School reserves the right to confiscate and search an iPad to ensure compliance with this Acceptable Use Policy

Staff Users must read and sign below:
I have read, understand, and agree to abide by the terms of the iPad Acceptable Use Policy.

Name	
Signature	
Date	

Penair School – CCTV Policy – Appendix 5

1. Aims

At Penair School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our schools and its members.
The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at our schools and ensure that:

- We comply with the UK GDPR, effective 25 May 2018.
- The images that are captured are useable for the purposes we require them.
- We assure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of CCTV systems which capture images of people who could be identified.

2. Legal Framework

This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The UK General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

This policy operates in conjunction with the following school policies:

- Photography and Videos at School Policy
- E-security Policy
- Freedom of Information Policy
- UK GDPR Data Protection Policy

3. Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **Surveillance** – monitoring the movements and behavior of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

Penair School does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances. Any areas covered by overt surveillance will be clearly signposted.

4. Roles and Responsibilities

The role of the data protection officer (DPO) includes:

- Offering advice to the data controller regarding processing surveillance and CCTV footage in accordance with data protection legislation.
- Reporting to the highest management level of the school, e.g. the governing board.
- Providing advise where requested regarding data protection impact assessment (DPIA) for CCTV.

The Head Teacher is the data controller. The governing body of Penair School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations. The DPO deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.

- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.

The role of the headteacher includes:

- Making decisions where CCTV is needed to justify its means.
- Seeking appropriate guidance with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

5. Purpose and Justification

The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors. Surveillance will be used as a deterrent for violent behavior and damage to the school. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any changing facility. If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them.

6. The Data Protection Principles

Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organizational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7. Objectives

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

8. Protocols

The surveillance system is a closed digital system. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.
The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.
The surveillance system will not be trained on individuals unless an immediate response to an incident is required. The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

9. Security

Access to the surveillance system, software and data will be strictly limited to authorized operators and will be password protected and those with authority to view CCTV data.

The school's authorised CCTV system operators are:

- IT Support Technicians
- ICT4

The school has authorised the following roles to make requests to view CCTV and view data Live:

- All members of the Senior Leadership Team.

The Head Teacher may authorise and document any additional person in the employment of Penair School to view CCTV data for a specific event related to an identified purpose of the system.

The main control facility is kept secure and locked when not in use. If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorization forms will be completed and retained. Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are always being properly maintained. Surveillance and CCTV systems will not be intrusive.

The DPO and headteacher will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders. Any unnecessary footage captured will be securely deleted from the school system. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach. Visual display monitors are located in the designated area.

10. Privacy by Design

The use of surveillance cameras and CCTV will be subject to a DPIA, in consultation with the DPO. A DPIA will be carried out prior to the installation of any surveillance and CCTV system.

If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues. Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

11. Code of Practice

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All surveillance footage will be kept for 28 days for security purposes; the headteacher and the data controller are responsible for keeping the records secure and allowing access. The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.
The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website. The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up to date.

12. Access

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed. All disks containing images belong to, and remain the property of, the school. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format. Requests by people outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the headteacher on a case-by-case basis with close regard to data protection and freedom of information legislation. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information. All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of receipt of the request. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry.
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

13. Monitoring and Review

This policy will be monitored and reviewed every year by the policyholder. The policyholder will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly. The policyholder will communicate changes to this policy to all members of staff.

Penair School – Cyber Response Plan – Appendix 6

1. Introduction

A Cyber Response Plan should be considered as part of an overall continuity plan that schools need to ensure they maintain a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

If a school fails to plan effectively then recovery can be severely impacted, causing additional loss of data, time, and ultimately, reputation.
Incidents may occur during the school day or out of hours. The Cyber Response Plan should be tested, with input from key stakeholders, to ensure that in an emergency there is a clear strategy, which has fail-safes when key personnel are unavailable.
The plan should cover all essential and critical IT infrastructure, systems, and networks. The plan will ensure that communications can be quickly established whilst activating cyber recovery. It is also important that the plan is well communicated and readily available.
The document is to ensure that in the event of a cyber attack, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

2. Aims of a Cyber Response Plan

When developing a Cyber Response Plan, you will need to consider who will be involved in the Cyber Recovery Team, the key roles and responsibilities of staff, what data assets are critical and how long you would be able to function without each one, establish plans for internal and *e*xternal communications and have thought about how you would access registers and staff and pupil contact details. This will allow the school:

- To ensure immediate and appropriate action is taken in the event of an IT incident.
- To enable prompt internal reporting and recording of incidents.
- To have immediate access to all relevant contact details (including backup services and IT technical support staff).
- To maintain the welfare of pupils and staff.
- To minimise disruption to the functioning of the school.
- To ensure that the school responds in a consistent and effective manner in order to reduce confusion and reactivity.
- To restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the school which are unaffected.

3. Cyber Response Insurance

The school holds Cyber Proactive Response Insurance through Howden UK Brokers Limited which is underwritten by CFC Underwriting Limited.

The comprehensive policy is designed to meet the insurance needs of companies with an exposure to cyber, privacy and media risks, including:

1. Cyber incident response costs to quickly neutralise or minimise the damage caused by a cyber event.
2. Cyber crime cover
3. Cover for system damage and business interruption caused by a cyber event
4. Network security, cyber and privacy liability cover
5. Cover for regulatory costs and fines
6. Cover for intellectual property infringement and defamation

Although there are no prerequisites needed to have cover in place with CFC Underwriting Limited, the school has ensured it meets the requirements that would be needed to qualify for the Risk Protection Cover (RPA) which requires member to meet the following things:

1. Have offline backups. Help and guidance on backing up is available from the National Cyber Security Centre (NCSC) and should ideally follow the 3-2-1 rule explained in the NCSC blog Offline backups in an online world - NCSC.GOV.UK

   It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups. Education providers should ask their IT teams or external IT providers to ensure the following:

   a) Backing up the right data. Ensuring the right data is backed up is paramount. A list of critical data is included in this Cyber Response Plan.

   b) Backups are held fully offline and not connected to systems or in cold storage, ideally following the 3-2-1 rule explained in the NCSC blog Offline backups in an online world: https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

   c) Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored, and data recovered from backups.

   Further Help and guidance on backing up can be found at: Step 1 - Backing up your data - NCSC.GOV.UK. https://www.ncsc.gov.uk/collection/small-businessguide/backing-your-data

2. All Employees or Governors who have access to the Member's information technology system must undertake NCSC Cyber Security Training annually. Training is available in the form of a video or as PowerPoint slides. Upon completion, a certificate can be downloaded by each person and staff must sign a declaration sheet to say they have completed the training. In the event of a claim the Member will be required to provide this evidence.

3. Register with Police CyberAlarm. Registering will connect Members with their local police cyber protect team and in the majority of cases, a cyber-alarm software tool can be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data. When registering, use the code “RPA Member” in the Signup code box

4. Have a Cyber Response Plan in place.

4.Preparation and Additional Resources

Preventative Strategies

It is vital education providers regularly review their existing defences and take the necessary steps to protect their networks. In addition to the 4 conditions of cover detailed above, there are several suggested measures that schools can implement to help themselves to improve their IT security and mitigate the risk of a cyber-attack:

Regularly review IT Security Policy and Data Protection Policy.

- Assess the school’s current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role based user access. Cyber Essentials is a government-backed baseline standard, which we would encourage all RPA members to strive towards achieving wherever possible.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user’s identity by using a combination of two or more different factors.
- Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis. Vulnerabilities within Microsoft Exchange Servers have been the root cause of many cyber-attacks in the last six months. It is highly recommended that on-premises exchange servers are reviewed and patched/updated as a high priority and moving to an Office 365 environment with MFA if possible.
- Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are:
    - If external RDP connections are used, MFA should be used
    - Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
    - Enable an account lockout policy for failed attempts
    - The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended

- Review NCSC advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks - NCSC.GOV.UK
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

Advice and guidance

- **The NCSC website has an extensive range of practical resources to help improve Cyber Security for Schools - NCSC.GOV.UK**

Acceptable Use

Ensure all users have read the relevant policies and signed IT acceptable use and loan agreements for school devices.

Please be aware if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the police.

Communicating the Plan

Communicate the Cyber Recovery Plan to all those who are likely to be affected and be sure to inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.

Testing and Review

During an incident there can be many actions to complete, and each step should be well thought out, cohesive, and ordered logically.

Train key staff members to feel confident following and implementing the plan. Review the plan regularly to ensure contact details are up-to-date and new systems have been included. NCSC have resources to test your incident response with an Exercise in a Box - NCSC.GOV.UK

Making Templates Readily Available

It is recommended that templates are available to cover reporting, recording, logging incidents and actions, and communicating to stakeholders.

5. Actions in the event of an incident

If you suspect you have been the victim of a ransomware or other cyber incident, you should take the following steps immediately:

- Enact your Cyber Recovery Plan
- Contact the 24/7/365 RPA Cyber Emergency Assistance:
    - By telephone: **0800 368 6378** or by email: **RPAresponse@CyberClan.com**
    - You will receive a guaranteed response within 15 minutes
    - Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible

    - Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including: forensic investigation services and support in bringing IT operations securely back up and running.
- Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
- Contact your local police via Action Fraud Action Fraud website or call **0300 123 2040**
- If you are a part of a Local Authority (LA), they should be contacted
- Contact your Data Protection Officer
- Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 1112**
- Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.

6. Cyber Recovery Plan

1. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
2. Assess and document the scope of the incident using the Incident Impact Assessment at Appendix A to identify which key functions are operational / which are affected.
3. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
4. In order to assist data recovery, if damage to a computer or back up material is suspected, staff **should not:**
    - Turn off electrical power to any computer.
    - Try to run any hard drive, back up disc or tape to try to retrieve data.
    - Tamper with or move damaged computers, discs or tapes.
5. Contact RPA Emergency Assistance Helpline.
6. Start the Actions Log to record recovery steps and monitor progress.
7. Convene the Cyber Recovery Team (CRT).
8. Liaise with IT staff to estimate the recovery time and likely impact.
9. Make a decision as to the safety of the school remaining open.
    - *This will be in liaison with relevant Local Authority Support Services / Trust*
10. Identify legal obligations and any required statutory reporting e.g., criminal acts / reports to the Information Commissioner's Office in the event of a data breach.
    - *This may involve the school's Data Protection Officer and the police*
11. Execute the communication strategy which should include a media / press release if applicable.
    - *Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.*

12. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
13. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix D and review the Cyber Recovery Plan accordingly.
14. Educate employees on avoiding similar incidents / implement lessons learned.

Ensure this plan is kept up-to-date with new suppliers, new contact details, and changes to policy.

Cyber Recovery Team

In the event of this plan having to be initiated, the personnel named below will form the Cyber Recovery Team and take control of the following:

	Name	Role in School	Contact Details
Recovery Team Leader	Headteacher	Headteacher	
Penair IT Strategic Lead	Penair IT Strategic Lead	Penair IT Strategic Lead	
Data Management	Data Manager	Data Manager	
IT Restore / Recover	IT Support Partner & Penair IT Support Technician	IT Support Partner Penair IT Support Technician	
Site Security	Business Manager/ /Site Manager	Business Manager/ /Site Manager	
Public Relations	Headteacher	Headteacher	
Communications	Headteacher	Headteacher	
Resources / Supplies	IT Support Partner Penair IT Support Technician	IT Support Partner Penair IT Support Technician	
Facilities Management	Business Manager /Site Manager	Business Manager /Site Manager	

This procedure should not be published with contact details included due to the risk of a data breach.

Server Access

Please detail all the people with administrative access to the server.

Role	Name	Contact Details
Headteacher	NA	NA
School Business Manager/Administrator	NA	NA
Penair IT Support Technician	Penair IT Support Technician	support@ict4.co.uk 01209 311344
Third Party IT Provider	ICT4 (IT Support Partner)	support@ict4.co.uk

		01209 311344

This procedure should not be published with contact details included due to the risk of a data breach.

Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Headteacher	NA	NA
School Business Manager/Administrator	NA	NA
MIS Provider	ESS	Sims Connected Support portal • **Telephone - 03330 150 212** • **Email - support@educationsoftwaresolutions.co.uk. Or log and view your cases via the Customer Support Portal.**
Data Manager	Data Manager	Penair School
Penair IT Support Technician	IT Support	Penair School

This procedure should not be published with contact details included due to the risk of a data breach.

In the event of a cyber incident, it may be helpful to consider how you would access the following:

- Registers
- Staff / Pupil contact details
- Current Child Protection Concerns

Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server	On-Site Backup to 2 different drives in separate building	Every 24 hours Monday To Friday
School MIS	Off-site By ESS	Daily snapshots. Continuous point in time recovery.
Cloud Services	Office 365	
Third Party Applications / Software	See SchoolPro Data Mapping	
Email Server	Office 365 Snap- shots & Barracuda through iCT4	14 Days Retained for 60 Days.

Curriculum Files	Office 365 Snap- shots & Barracuda through iCT4	12 Hours Retained for 60 Days.
Teaching Staff Devices	Office 365 Snap- shots & Barracuda through iCT4	12 Hours Retained for 60 Days.
Administration Files	Office 365 Snap- shots & Barracuda through iCT4	12 Hours Retained for 60 Days.
Finance / Purchasing	Off-site By ESS	Daily snapshots. Continuous point in time recovery.
HR / Personnel Records	Sam People	Daily snapshots. Continuous point in time recovery. Synced every 6 mins
Inventory	Every Education – off site	
Facilities Management / Bookings	Every Education – off site / TES Global – Room Booking System	
Website	Lbcreative.co.uk – off site	Hosted by R M Education Limited – off site
USBs / portable drives	**These should not be in use**	

Key Contacts

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection	01209 311344	ICT4 Penair
Backup Provider	01209 311344	Barracuda through ICT4
Telecom Provider	01209 311344	Office 365 Teams through ICT4
Website Host	01235 645317	R M Education Ltd
Electricity Supplier	0800 130 3600 / 0800 804 8589	Engie and Corona
Burglar Alarm	01726 65636	Waldon Security
Text Messaging System	https://class-charts.help.tes.com/support/tickets/new support.classcharts@tes.com	Class Charts Communications
Action Fraud	0300 123 2040	https://www.reportfraud.police.uk
Local Constabulary	101	Devon and Cornwall Police https://safercornwall.co.uk/cyber-crime
Legal Representative	0330 045 2808	Browne Jacobson

LA / Trust Press Officer	0300 123 4100	Cornwall Council Media Team

This procedure should not be published with contact details included due to the risk of a data breach.

Staff Media Contact

The Headteacher is the assigned media contact and they will co-ordinate with the media, working to guidelines that have been previously approved for dealing with post-disaster communications. The Headteacher may delegate this responsibility during a cyber incident but will retain oversight. The Headteacher or their delegate will only provide verified facts. It is likely that verifying details will take some time and stating, "I don't know at this stage", is a perfectly acceptable response. It is likely the following basic questions will form the basis of information requests:

- What happened?
- How did it happen?
- What are you going to do about it?

Staff who have not been delegated responsibility for media communications **should not respond** to requests for information and should refer callers or media representatives to assigned staff.

Key Roles and Responsibilities

Headteacher (with support from Deputy Headteacher/ IT Strategic Lead)

- Seeks clarification from person notifying incident.
- Sets up and maintains an incident log, including dates / times and actions.
- Convenes the Cyber Recovery Team (CRT) to inform of incident and enact the plan.
- Liaises with the Chair of Governors.
- Liaises with the school Data Protection Officer (SchoolPro).
- Convenes and informs staff, advising them to follow the 'script' when discussing the incident.
- Prepares relevant statements / letters for the media, parents / pupils.
- Liaises with School Business Officer / Manager to contact parents, if required, as necessary

Designated Safeguarding Lead (DSL)

- Seeks clarification as to whether there is a safeguarding aspect to the incident.
- Considers whether a referral to Cyber Protect Officers / Early Help / Social Services is required.

Site Manager / Caretaker

- Ensures site access for external IT staff.
- Liaises with the Headteacher to ensure access is limited to essential personnel.

School Business Manager/Administrator

- Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
- Ensures office staff understand the standard response and knows who the media contact within school is.
- Contacts relevant external agencies – RPA Emergency Assistance / IT services / technical support staff
- Manages the communications, website / texts to parents / school emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

Data Protection Officer (DPO- SchoolPro Tlc)

- Supports the school, using the school data map and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- Liaises with the Headteacher / Chair of Governors and determines if a report to the ICO is necessary.
- Advises on the appropriateness of any plans for temporary access / systems.

IT Provider (ICT4)

- Verifies the most recent and successful backup.

- Liaises with the RPA Incident Response Service to assess whether the backup can be restored or if server(s) themselves are damaged, restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss.
- Liaises with the Headteacher as to the likely cost of repair / restore / required hardware purchase.
- Provides an estimate of any downtime and advises which systems are affected / unaffected.
- If necessary, arranges for access to the off-site backup.
- Protects any records which have not been affected.
- Ensures on-going access to unaffected records.

Teaching Staff and Teaching Assistants

- Reassures pupils, staying within agreed pupil standard response
- Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed

Critical Activities - Data Assets

List all the data assets your school has access to and decide which are critical and how long you would be able to function without each one. This could be a matter of a few hours or a matter of a day, a week or even a month.

Complete the required column with the timescale you believe is necessary for recovery. You may find it helpful to refer to your Inventory / Data Map.

Assign: 4 hours / 12 hours / 24 hours / 48 hours / 72 hours / 1 week / 2 weeks / 3 weeks / 1 month

Also decide if there are any temporary workarounds or if outsourcing is possible. It is useful to consider the cost of any additional resources which may be required in an emergency situation.

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Leadership and Management	Access to Headteacher's email address	**24 hours**	No
	Minutes of SLT meetings and agendas	**1 week**	No
	Head's reports to governors (past and present)	**1 week**	Yes
	Key stage, departmental and class information	**1 week**	Yes
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns	**4 hours**	No
	Attendance registers	**4 hours**	Yes (pdf backups termly)
	Class groups / teaching groups, and staff timetables	**12 hours**	Yes (pdf backups termly)
	Referral information / outside agency / TAFs	**12 hours**	Yes (Agency)
	Child protection records	**12 hours**	Yes (LA)
	Looked After Children (LAC) records / PEPs	**12 hours**	Yes (LA)
	Pupil Premium pupils and funding allocations	**1 week**	Yes (GIAP)
	Pastoral records and welfare information	**12 hours**	No
Medical	Access to medical conditions information	**4 hours**	Yes
	Administration of Medicines Record	**4 hours**	Yes
	First Aid / Accident Logs	**1 week**	Yes (offsite Backups)
Teaching	Schemes of work, lesson plans and objectives	**72 hours**	Yes (offsite Backups)
	Seating plans	**72 hours**	Yes (offsite Backups)
	Teaching resources, such as worksheets	**72 hours**	Yes (offsite Backups)
	Learning platform / online homework platform	**1 week**	Yes (offsite Backups)
	Curriculum learning apps and online resources	**1 week**	Yes (offsite Backups)
	CPD / staff training records	**1 month**	Yes (offsite Backups)
	Pupil reports and parental communications	**48 hours**	Yes (email Backups)
SEND Data	SEND List and records of provision	**24 hours**	Yes (Paper Files)
	Accessibility tools	**12 hours**	No
	Access arrangements and adjustments	**4 hours**	Yes
	IEPs / EHCPs / GRIPS	**12 hours**	Yes (LA)
Conduct and Behaviour	Reward system records, including house points or conduct points	**72 hours**	Yes (Class Charts offsite)

	Behaviour system records, including negative behaviour points	**72 hours**	Yes (Class Charts offsite)
	Sanctions	**24 hours**	Yes (Class Charts offsite)
	Exclusion records, past and current	**72 hours**	Yes (Class Charts offsite)
	Behavioural observations / staff notes and incident records	**72 hours**	Yes (Class Charts offsite)
Critical Activities	**Data item required for service continuity**	**When Required**	**Workaround? (Yes / No)**
Assessment and Exams	Exam entries and controlled assessments	**12 hours**	Yes (Exam boards)
	Targets, assessment and tracking data	**1 month**	Yes
	Baseline and prior attainment records	**1 month**	Yes
	Exam timetables and cover provision	**12 hours**	Yes (offsite backups)
	Exam results	**1 month**	Yes (Exam boards)
Governance	School development plans	**1 week**	Yes
	Policies and procedures	**12 hours**	Yes (offsite backups)
	Governors meeting dates / calendar	**1 week**	Yes (offsite backups)
	Governor attendance and training records	**1 week**	Yes (offsite backups)
	Governors minutes and agendas	**48 hours**	Yes (offsite backups)
Administration	Admissions information	**1 week**	Yes (Admissions+)
	School to school transfers	**1 week**	No
	Transition information	**1 week**	Yes (Primary Schools)
	Contact details of pupils and parents	**4 hours**	Yes (restore access to SIMS/ Class charts)
	Access to absence reporting systems	**4 hours**	Yes (paper registers then restore access to SIMS/ Class charts)
	School diary of appointments / meetings	**12 Hours**	Yes
	Pupil timetables	**4 hours**	Yes (pdf backups termly)
	Letters to parents / newsletters	**1 week**	Yes
	Extra-curricular activity timetable and contacts for providers	**1 week**	Yes
	Census records and statutory return data	**1 week**	Yes (DfE)
Human Resources	Payroll systems	**48 hours**	Yes (LA)
	Staff attendance, absences, and reporting facilities	**1 week**	Yes (SAM People)
	Disciplinary / grievance records	**1 month**	Yes (Paper Records)
	Staff timetables and any cover arrangements	**4 hours**	Yes (restore access to SIMS)
	Contact details of staff	**4 hours**	Yes (SAM People)
	Photocopying / printing provision	**4 hours**	Yes

Office Management	Telecoms - school phones and access to answerphone messages	**12 hours**	No
	Email - access to school email systems	**24 hours**	No
	School website and any website chat functions / contact forms	**24 hours**	No
	Social media accounts (Facebook / Twitter)	**4 hours**	No
	Management Information System (MIS)	**12 hours**	No
	School text messaging system (Class Charts)	**12 hours**	Yes
	School payments system (for parents)	**12 hours**	Yes
	Financial Management System - access for orders / purchases	**12 hours**	Yes (FMS offsite)
Site Management	Visitor sign in / sign out	**4 hours**	Yes
	CCTV access	**1 week**	No
	Site maps	**4 hours**	Yes (offsite Backups)
	Maintenance logs, including legionella and fire records	**1 week**	Yes (off site systems)
	Risk assessments and risk management systems	**1 week**	Yes (Local Authority offsite)
	COSHH register and asbestos register	**1 week**	Yes (Local Authority offsite)
Catering	Contact information for catering staff	**4 hours**	Yes (3rd party contractor)
	Supplier contact details	**12 hours**	Yes (3rd party contractor)
	Payment records for food & drink	**12 hours**	Yes (restore access to SCOPAY)
	Special dietary requirements / allergies	**4 hours**	Yes (3rd party contractor)
	Stock taking and orders	**12 hours**	Yes (3rd party contractor)

Appendix A: Incident Impact Assessment

Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

Operational	No Impact	There is no noticeable impact on the school's ability to function.
	Minor Impact	There is some loss in the ability to function which is minor. Functions can be carried out, but may take longer and there is a loss of efficiency.
	Medium Impact	The school has lost the ability to provide some critical services (administration **or** teaching and learning) to **some** users. The loss of functionality is noticeable, but work arounds are possible with planning and additional resource.
	High Impact	The school can no longer provide any critical services to users. It is likely the school will close or disruption will be considerable.

Informational	No Breach	No information has been accessed / compromised or lost.
	Data Breach	Access or loss of data which is **not** linked to individuals and classed as personal. This may include school action plans, lesson planning, policies and meeting notes.
	Personal Data Breach	Sensitive personally identifiable data has been accessed or extracted. Data which may cause 'significant impact' to the person / people concerned requires a report to the ICO within 72 hours.
	Integrity Loss	Data, which may include sensitive personal data, has been changed or deleted. (This also includes corruption of data)

Restoration	Existing Resources	Recovery can be promptly facilitated with the resources which are readily available to the school.
	Facilitated by Additional Resources	Recovery can be facilitated within an identified timescale with additional resources which can be easily accessed.
	Third Party Services	Recovery is not guaranteed, and outside services are required to facilitate full or partial restoration.
	Not Recoverable	Recovery from the incident is not possible. Data may have been extracted, encrypted or backups may have failed.

Appendix B: Communication Templates

1. School Open

Dear Parent/Carer,
I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down [some / all] of the school IT systems. This means that we currently do not have any access to [telephones / emails / server / MIS etc] At present we have no indication of how long it will take to restore our systems. [OR it is anticipated it may take XXXX to restore these systems]
We are in liaison with our school Data Protection Officer and, if required, this data breach will be reported to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / GDPR. Every action has been taken to minimise disruption and data loss.
The school will be working with the [Trust / Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and normal working as soon as possible.
In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff. The school will remain open with the following changes [detail any changes required]
I appreciate that this will cause some problems for parents/carers with regards to school communications and apologise for any inconvenience.
We will continue to assess the situation and update parents/carers as necessary. [If possible, inform how you will update i.e. via website/text message]
Yours sincerely,

2. School Closure

Dear Parent/Carer,
I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down the school IT system. This means that we currently do not have any access to [telephones / emails / server / MIS etc]. At present we have no indication of how long it will take to restore our systems.
We are in liaison with our school Data Protection Officer and this data breach has been reported to the Information Commissioners Office (ICO) in line with the requirements of the Data Protection Act 2018 / GDPR.
In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff.
I feel that we have no option other than to close the school to students on [XXXXXXXXXX]. We are currently planning that the school will be open as normal on [XXXXXXXXXX]
I appreciate that this will cause some problems for parents/carers with regards to childcare arrangements and apologise for any inconvenience but feel that we have no option other than to take this course of action.
The school will be working with the [Trust / Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and re-open as soon as possible.
We will continue to assess the situation and update parents / carers as necessary. [If possible, inform how you will update i.e. via website / text message].
Yours sincerely,

3. Staff Statement School Open

The school detected a cyber-attack on [date] which has affected the following school IT systems:
(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will remain open with the following changes to working practice:
(Detail any workarounds / changes)

The school is in contact with our Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.
This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, limit severity, and restore systems.
All staff are reminded that they must not make any comment or statement to the press, parents or wider community with regards to this incident or its effects. Queries should be directed to [Insert staff name]

4. Staff Statement School Closed

The school detected a cyber-attack on [date] which has affected the following school IT systems: (Provide a description of the services affected)
Following liaison with the [Trust / LA] the school will close to pupils [on DATE or with immediate effect].
(Detail staff expectations and any workarounds / changes or remote learning provision)
The school is in contact with our Data Protection Officer, and we have reported the incident to the ICO, in line with the statutory requirements of the Data Protection Act 2018 / GDPR.
This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, however we are unsure when systems will be restored. Staff will be kept informed via [telephone / email / staff noticeboard].
All staff are reminded that they must not make any comment or statement to the press, parents, or wider community with regards to this incident or its effects. Queries should be directed to [Insert staff name].

5. Media Statement (from Headteacher only)

[Inset school name] detected a cyber-attack on [date] which has affected the school IT systems. Following liaison with the [Trust / LA] the school [will remain open / is currently closed] to pupils.

The school is in contact with their Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities and the school has taken immediate remedial action to limit data loss and restore systems.

A standard staff response for serious IT incidents should reflect only information which is already freely available and has been provided by the school in initial media responses.

Standard Response

The information provided should be factual and include the time and date of the incident.

Staff should not speculate how long systems will take to be restored but can provide an estimate if this has been agreed.

If no restoration date has been advised, staff should merely state that work is on-going and that services will resume as soon as practically possible.

Staff should direct further enquiries to an assigned contact / school website / other pre-determined communication route.

Standard Response for Pupils

For staff responding to pupil requests for information, responses should reassure concerned pupils that incidents are well prepared for, alternative arrangements are in place and that systems will be back online shortly.

Staff should address any outlandish or suggested versions of events by reiterating the facts and advising pupils that this has been confirmed in letters / emails to parents / carers.

Staff should not speculate or provide pupils with any timescales for recovery, unless the sharing of timescales has been authorised by senior staff.

Appendix C: Incident Recovery Event Recording Form

This form can be used to record all key events completed whilst following the stages of the Cyber Response Plan.

Description or reference of incident:	
Date of the incident:	
Date of the incident report:	
Date/time incident recovery commenced:	
Date recovery work was completed:	
Was full recovery achieved?	

Relevant Referrals

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

Actions Log

Recovery Tasks (*In order of completion)*	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

Appendix D: Post Incident Evaluation

Response Grades 1-5 1 = Poor, ineffective and slow / 5 = Efficient, well communicated and effective.

Action	Response Grading	Comments for Improvements / Amendments
Initial Incident Notification		
Enactment of the Action plan		
Co-ordination of the Cyber Recovery Team		
Communications Strategy		
Impact minimisation		
Backup and restore processes		
Were contingency plans sufficient?		
Staff roles assigned and carried out correctly?		
Timescale for resolution / restore		
Was full recovery achieved?		
Log any requirements for additional training and suggested changes to policy / procedure:		

Document control				
Approved by	Business, Audit & Risk Committee			
Published location	Website	**Next Review**	**Policy Holder** Summer 2027	**Governing Board (annual)** Summer 2027
Version Number	**Date issued**	**Author**	**Changes**	
2	Summer 2026	Sally Wood	Version control Implemented	
2	Summer 2026	Tony Hill	Policyholder annual review Addition of appendices	