



PENAIR
SCHOOL



IT Services Information Security Policy

Policy holder:	Business Manager
----------------	------------------

To be reviewed by policy holder:	Annually
----------------------------------	----------

Last reviewed by the Governing Board:	Autumn 2025
---------------------------------------	-------------

Next review by the Governing Board:	Autumn 2026
-------------------------------------	-------------

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	5
12	Responsibilities	5

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 Teachers 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 School's 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 or 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.
- 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	<p>Responsible for:</p> <ul style="list-style-type: none"> • 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	<p>The School's Leadership Team supported by the IT Manager ensures that security is properly evaluated and managed across the School.</p> <p>IT Governance is responsible for:</p> <ul style="list-style-type: none"> • 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	http://www.legislation.gov.uk/uksi/2000/2699/contents/made
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