Pittville School
learning to achieve

# Information & Cyber Security Policy

| | | | |
|---|---|---|---|
| **Approved by:** | [Finance and Premises Portfolio] | **Date:** [1 February 2023] | |
| **Last reviewed on:** | [January 2023] | | |
| **Next review due by:** | [January 2026] | | |

**Dissemination of the Policy: All staff and Governors, School Website**

**History of policy changes**

| Date | Version | Change | Origin of change e.g. change in legislation, request by TU | Changed by |
|---|---|---|---|---|
| Jan 23 | | Include Cyber Security | | |
| | | | | |
| | | | | |

## Contents

## 1 Purpose

Information that is collected, analysed, processed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

Information may be put at risk by poor education and training, and the breach of security controls.

Information or Cyber security incidents can give rise to reputational damage, financial loss, non-compliance with standards and legislation as well as civil and / or criminal liability.

This Information & Cyber Security Policy sits alongside other school policies, mainly:

- Data Protection Policy; and
- On-line Safety Policy
- Clean Desk Policy
- Critical Incident Policy
- Information and Records Retention Policy

## 2 Objectives

The School's security objectives are that:

- Our information risks are identified, managed and treated according to an agreed risk tolerance
- Our authorised users can securely access and share information in order to perform their job roles
- Our physical, procedural and technical controls balance user experience with the required security
- Our contractual and legal obligations relating to information security are met
- Our teaching and administrative activity considers information security
- Individuals accessing our information are aware of their information security responsibilities
- Incidents affecting our information assets are reported, investigated, resolved, and learnt from to improve our controls

## 3 Scope

The Information & Cyber Security Policy and its supporting controls, processes and procedures apply to all information used at the School, in all formats. This includes information processed by other organisations in their dealings with the School.

The Information & Cyber Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to School information and technologies, including external parties that provide information processing services to the School.

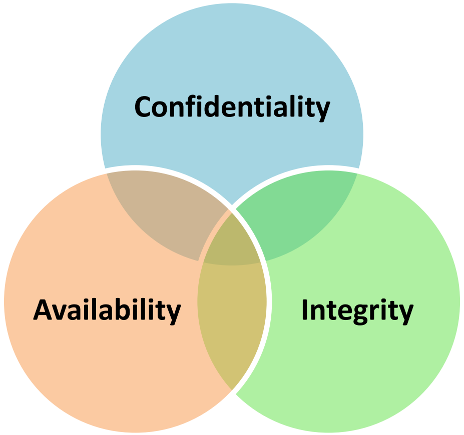
## 4 Review

A review of this policy will be undertaken by the Schools Senior Management Team annually or more frequently as required, and will be approved by the Governing Body.

## 5 Policy Declaration

It is the School's policy to ensure that information is protected from a loss of:

- **Confidentiality** – information will be accessible only to authorised individuals
- **Integrity** – the accuracy and completeness of information will be maintained
- **Availability** – information will be accessible to authorised users and processes when required



It will be the responsibility of all stakeholders to ensure confidentiality and availability of electronic information. However, the school's IT service provider will take a leading role in ensuring this is met.

The school will take responsibility for data integrity, ensuring data should be intact, accurate and complete. The IT managed service provider will support the school in ensuring the integrity of data, in that it must protect the data on the systems it manages.

## 6 Information Security Framework

A set of lower-level controls, processes and procedures for information security will be defined, in support of the Information Security Policy and its stated objectives. This suite of supporting documentation will be approved by the Senior Management Team, published, and communicated to School's users and relevant external parties.

## 7 Asset Management

All assets (information, software and electronic information processing equipment) will be documented and accounted for. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

All information assets will be classified according to their legal requirements, business value, criticality and sensitivity, and classification will indicate appropriate handling requirements. All information assets will have a defined retention and disposal schedule.

## 8 Access Control

Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed, and will include consideration of multiple factor authentication as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

Access control mechanisms will apply to both electronic and physical access to data and information.

## 9 Cryptography

The School will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

## 10 Physical and Environmental Security

Data (at rest) and being processed are housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible attack.

## 11 Personnel Security

The school will endure the correct and secure operations of information processing systems.

This will include;

- Data access controls
- Physical access and location access controls
- Appropriate training for cyber security behaviours and expectations
- Acceptable Use Policies for all students, parents, staff, governors and visitors

## 12 Operations Security

The School will ensure the correct and secure operations of information processing systems.

This will include:

- Documented operating procedures
- The use of formal change management
- Controls against viruses, malware and ransomware
- Defined use of logging/monitoring

## 13 Network Security

The School will maintain network security controls to ensure the protection of information within its networks, and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

## 14 Supplier Relationships

The school's information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected.

Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

Management of the supplier relationship will be governed by the Managed Service Agreements and associated service level agreements signed with the supplier along with regular service review meetings as necessary.

## 15 Protection from Cyber Attacks

Please see the glossary (appendix 1) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure from cyber attack
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Update or replace software in response to known vulnerabilities
- Not engage with ransom requests in the event of a ransomware attack, as this would not guarantee recovery of data
- Put controls in place that are:
  - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
  - Up to date: with a system in place to monitor when the school needs to update its software
  - Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be
- Back up critical data nightly and store these backups on network storage and then to a secure cloud storage facility with limited access.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department in conjunction with Gloucester County Councils Schools IT department.
- Require staff to:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Enable multi-factor authentication where they can, on things like school email accounts

- Conduct regular access reviews to make sure each user in the school has the right level of access permissions
- Have an effective firewall in place
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification where appropriate
- Work with Gloucester County Council to adopt emerging leading practices relating to cyber security, such as advice on which service providers to use or assistance with procurement in accordance with the school's Critical Incident Policy.

## 16 Information Security Incident Management

The school will ensure that there are appropriate detective and corrective controls in place e.g. maintain system logs, filtering alerts, Microsoft alerts that highlight unusual activity. There are active corrective controls e.g. geolocation blocks therefore controlling access that is proactively therefore preventing and protecting once detected. Guidance will be available on what constitutes an Information Security incident and how this should be reported.

Actual or suspected breaches of information security must be reported to the schools data protection officer (DPO) and will be investigated.

Appropriate corrective action will be taken and any learning built in to controls.

## 17 Training and Awareness

Ongoing training and awareness programmes will be provided to help employees understand and comply with this policy. These programmes may include in-person training, online resources, and simulated phishing attacks. The school requires users to report any suspicious emails or other potential threats to the IT support provider for investigation/remediation.

## Appendix 1: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

| TERM | DEFINITION |
|---|---|
| **Antivirus** | Software designed to detect, stop and remove malicious software and viruses. |
| **Breach** | When your data, systems or networks are accessed or changed in a non-authorised way. |
| **Cloud** | Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices. |
| **Cyber attack** | An attempt to access, damage or disrupt your computer systems, networks or devices maliciously. |
| **Cyber incident** | Where the security of your system or service has been breached. |
| **Cyber security** | The protection of your devices, services and networks (and the information they contain) from theft or damage. |
| **Download attack** | Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent. |
| **Firewall** | Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network. |
| **Hacker** | Someone with some computer skills who uses them to break into computers, systems and networks. |
| **Malware** | Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations. |
| **Patching** | Updating firmware or software to improve security and/or enhance functionality. |
| **Pentest** | Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses. |
| **Pharming** | An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address. |
| **Phishing** | Untargeted, mass emails sent to many people asking for sensitive information (such as bank |

| TERM | DEFINITION |
|---|---|
| | details) or encouraging them to visit a fake website. |
| **Ransomware** | Malicious software that stops you from using your data or systems until you make a payment. |
| **Social engineering** | Manipulating people into giving information or carrying out specific actions that an attacker can use. |
| **Spear-phishing** | A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts. |
| **Trojan** | A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer. |
| **Two-factor/multi-factor authentication** | Using 2 or more different components to verify a user's identity. |
| **Virus** | Programmes designed to self-replicate and infect legitimate software programs or systems. |
| **Virtual private network (VPN)** | An encrypted network which allows remote users to connect securely. |
| **Whaling** | Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation. |