# IT Services Governance

# Information Security Policy

Sheldon School

BE KIND | BE BRAVE | BE THE BEST YOU

## Working in partnership with

DATA PROTECTION EDUCATION

| | |
|---|---|
| Leadership Responsibility: **Chief Operating Officer** | Effective Date: **October 2025** |
| Governors' Committee Responsible: **Resources** | Review Date: **October 2026** |

# Contents

# Introducing our Information Security Policy

Sheldon's Leadership Team is fully committed to protecting organisation information systems. This Information Security Policy is an overarching policy that defines Sheldon's approach on how risks are managed within the organisation to keep information secure, meet legal and regulatory requirements and support strategic goals.

This Information Security Policy applies to all staff, temporary workers, contractors, interns, volunteers, governors and third parties who have access to or are processing the organisation's information in all formats. This includes all forms of paper, electronic and verbal information.

# Definitions

Information Security has three main principles, confidentiality, integrity and availability. Collectively, these principles are also known as the CIA triad.

| | |
|---|---|
| **Confidentiality (C)** | Information must be kept confidential; the data must be protected from unauthorised access. |
| **Integrity (I)** | Information must not be changed in an unauthorised manner and the information stored is correct. |
| **Availability (A)** | Information must be available when it is needed |
| **CIA Triad** | Information Security has three main principles, confidentiality, integrity and availability. Collectively, these principles are also known as the CIA triad. Each principle needs to be considered together to secure information, especially when creating or changing systems, processes or when carrying out a security audit or review. |
| **Incident** | An incident is a successful attempt to either impact the confidentiality, integrity or availability of data |
| **Event** | An event is an unsuccessful attempt to impact the confidentiality, integrity or availability of organisation's data |
| **Information Asset** | An information asset can be a paper document, a digital document, a database or any other type of digital file that the organisation considers has value. |
| **Physical Asset** | A physical device such as a laptop, PC, WIFI router, server, mobile, USB stick, external memory drive, printer (with memory), or any other physical device that stores organisation information |

# Objectives

The organisation's information security objectives are to:

- Prevent unauthorised access to organisation's confidential information
- Ensure that organisation information is accurate and that it cannot be modified in an unauthorised manner
- Ensure that the organisation information can be available when it is needed
- Our information risks are identified, managed and treated according to an agreed risk tolerance
- Be aware of the organisation's threat landscape by logging all CIA incidents and events
- Ensure that all individuals have a good understanding of Information Security awareness, which can be seen in their behaviours
- Meet regulatory requirements

# Roles and Responsibilities

The organisation will define and implement suitable governance procedures to manage information security risk by allocating security responsibilities to relevant individuals.

- The Director of IT Services is accountable for the organisation's information security.
- The Resources Committee are responsible to review, influence, implement continual improvement and to promote information security awareness within the organisation. The Resources Committee are responsible for continual improvement, approving the implementation of new policies and procedures and making changes to them.
- Information Asset Owners are accountable for the organisation's information assets. They will ensure that their information assets are kept up to date, accessed only by individuals who needs the information to perform their role and protected securely throughout the information assets lifecycle (when it is created, stored, transferred and deleted) and will assess and manage any risks to the asset.

# Network and IT System Security

The Director of IT Services is responsible to secure and manage the organisation's network. Their responsibilities shall include identifying threats and vulnerabilities to the network, the implementation of continual improvements, the audit and monitoring of the organisation's information systems and fixing any issues identified.

Connection to the network is only allowed after a user registration has been approved.

# Risk Management

Sheldon has a risk management process in place and has defined their risk appetite level. The level of security controls placed on organisation information depends on the confidentiality and sensitivity of the data.

Risk assessments are carried out on the organisation's information with the introduction of a new system that will process or store information when a change to an information system takes place when a new information asset is introduced or on an annual basis.

Resources who understand least privileged access, segregation of duty, use of appropriate technical security controls and data protection legislation should take part in these risk assessments to support the identification of all threats and vulnerabilities to the information asset.

A risk score is calculated from likelihood x impact = risk score

A treatment is defined for each risk which could either be to:

- Accept the risk
- Mitigate the risk
- Transfer the risk
- Avoid the risk.

All risks must be documented in the risk register, which is stored securely and accessed only by individuals who need access to perform their role. High risks and oldest risks are assessed by the Leadership Team on a regular basis.

Personal data that is regulated by Data Protection regulations must be treated in accordance with those regulations. Sensitive data must be risk assessed based on the fact that under the DPA 2018 and UK GDPR that type of data requires a higher level of security controls in place.

# Access Control

All staff members have been issued with an Access Card that gives them the ability to access the organisation premises.

There must be a user registration and de-registration procedure in place to ensure appropriate access control. This must include when an individual starts working at the organisation, moves roles within the organisation and leaves the organisation.

Access to organisation information will be defined by least privilege, access to information is granted based on the information that an individual needs to perform their role.

Individuals are responsible for their own accounts, they must not write down, share or disclose their password to any other third party. Passwords must be at least 10 characters long in accordance with the Password Policy and two-factor authentication should be used where it is available.

Remote access to organisation information must be encrypted and authorised in a secure manner, either via a Virtual Private Network (VPN) or by accessing secure organisation online software applications that are HTTPS and have two-factor authentication in place.

The Bring Your Own Device Policy defines further details about using personal devices to access organisation information systems.

Administration accounts must only be used for administration purposes. Segregation of duties will be implemented, where practical.

# Data Classification

There are four levels of data classification in place within the organisation.

| | |
|---|---|
| **Public** | Information that is allowed to be shared with everyone. Non-sensitive information that is available for public disclosure. The impact of unauthorized disclosure **does not harm the organisation**.<br><br>e.g. Newsletters or information published on the website. |
| **Internal** | Information that can be shared internally with all staff, but is protected with limited control. The unauthorized disclosure of information here can cause **limited harm** to the organisation.<br><br>e.g. Organisation charts, internal telephone directory. |
| **Private** | Information belonging to the organisation and not for disclosure to the public and that has restricted access. The unauthorized disclosure of information here can cause **moderate harm** to the organisation.<br><br>e.g. planning documents, attendance records |
| **Confidential** | The information which is very sensitive or private, of highest value to the organisation and intended to use by named individuals only. **The unauthorized disclosure of such information can cause severe harm** (e.g. legal or financial liability, reputational damage).<br><br>e.g. pupil safeguarding data, employee payroll data |

Any copying or distribution of either private or confidential information must be done in accordance with the organisation information handling process and recorded where necessary.

# Information Asset Management

All information assets must be labelled with the appropriate data classification where ever possible and recorded in an information asset register.

The Information Asset register includes the name of the asset, the owner, which systems the asset is stored in, which organisational roles access the asset, its data classification, what format it's in, whether the asset includes personal data, whether it is a critical asset and the risk score associated with the asset. This is updated when the details of an information asset changes the ownership of the asset changes, it is discontinued to be used or a new information asset is introduced.

On the Data Protection Education Knowledge Bank, the Information Asset Register is a function of the Record of Processing tool.

**Software Management**

Only approved software is allowed to be used to work with organisation data and be installed on organisation devices. The Director of IT Services has a list of approved software and firmware, including versions and licenses in place that is allowed to be used by the organisation.

Software that hasn't been approved and on this list is not allowed to be installed on organisation devices without gaining approval after going through the change management process.

# Physical Asset Management

Laptops and PCs must be configured with device encryption in place, firewalls turned on, antimalware installed, and configured to lock after 15 minutes of non-use with the password set up according to the organisation's password policy.

Mobile devices must use a 6-digit pin, finger or facial recognition.

Only organisation purchased removable media devices are allowed to be used on organisation owned devices in exceptional circumstances and for specified purposes. Any transfer of organisation confidential or private data to removable media must be approved, recorded and the device must be encrypted.

Physical devices must be securely wiped prior to disposal, using appropriate tools that do not allow the retrieval of data. Confidential or Private documents must be disposed of in a cross shredder.

All physical assets must be recorded and kept up to date in the organisation's asset register.

Physical documents, taken off school premises and all confidential documents within the school should be logged out of their permanent filing location and signed back in with the shortest practicable timeframe. The security of this document is the responsibility of the person signing for the document during this time frame.

The physical asset register includes make and model, the owner, operating system, location of the asset and date of ownership. This is updated when an asset is no longer being used, the owner has changed or a new asset is purchased. The asset register should also include any personal devices used as 'bring your own devices' which are configured or which are able to access organisation information.

A Clear Desk Approach should be adhered to ensure that internal, private and confidential documents are stored securely when not in use.

# Patch Management

It is very important for the organisation to keep all software up to date as vulnerabilities can be identified and potentially exploited.

Software patches must be kept up to date and set to automatically deploy where possible and appropriate.

The below targets have been defined for the deployment of patches based on their severity.

- **Critical** Implemented automatically or within **[3]** working days
- **High** Implemented automatically or within **[5]** working days
- **Medium** Implemented automatically or within **[10]** working days
- **Low** Implemented automatically or within **[2]** months

# Incident Management

An incident response process must be in place to identify and log events and incidents that impact the CIA or the organisation's information systems. If an incident is identified as a data breach, the Data Breach Process must be followed. These incidents and their root causes must be reviewed on a regular basis with the Leadership Team to assess the threat landscape of the organisation, identify any risks and implement security controls for continual improvement

# Logging and Monitoring

The organisation must have the ability to review user access logs to key systems that store personal, sensitive, private or confidential information. The logs must not be able to be modified.

An incident response process must be in place to identify and log events and incidents that impact the CIA of the organisation's information systems.

These must be reviewed once incidents have been logged as closed and all incidents must be reviewed on an annual basis with the Leadership Team to assess the threat landscape of the organisation, patterns of risk, and to identify any risks and implement security controls for continual improvement.

# Change Management

Sheldon School has defined a governance process for change. All changes to information systems are risk assessed and go through an approval process prior to the change being implemented. Change and risk can be documented in the Record of Processing tool.

# Managing Human Risk

The prime and most successful target vector to breach data is people. This highlights the importance of all organisation staff having a high level of information security awareness.

All staff members, governors and auxiliary staff who have access to organisation information must receive security awareness training on induction and on a yearly basis.

All staff members, contractors, interns and volunteers must be vetted appropriately, references gathered and DBS checks made where required, prior to commencing work in the organisation.

# Operations and Documentation

All information security standards and procedures will be documented where appropriate. This shall include but is not limited to:

- Firewall configurations
- Server configuration or image
- Laptop configuration or image
- Mobile device configuration
- WIFI router configuration

# Third Parties

Appropriate contractual agreements must be in place with all third parties who have access to or process organisation information.

Third-party access to organisation information must be based on least privilege, they should have access to the least amount of organisation information that they need to perform their services.

Prior to agreeing to a new third party accessing or processing organisation information, the third party must be risk assessed to ensure that that the information will be secure and processed in line with any relevant regulations, such as the Data Protection Act 2018 and UK GDPR.

This due diligence should take place on an annual basis to assess whether the security controls in place have been changed or are still considered to be secure.

Where appropriate, changes will be shared with internal or external interested parties in accordance with our privacy policy, contracts and data protection regulations.

# Physical Security

Appropriate physical security controls must be in place to restrict access to the building to prevent unauthorised access to the organisation such as an ID swipe entry system that only allows access for members of staff, CCTV, intercoms, locked and gated organisation grounds etc.

Staff must have a visible identifier to show that they are a member of staff, such as a lanyard or sticker/badge.

All visitors must document their name, the date and time of their visit, the purpose of their visit, who they are coming to meet with, wear either a lanyard or sticker/badge to highlight to other members staff and children that they are a visitor and be accompanied around the organisation. If the visitor requires access to organisation data, ensure that their identity is confirmed prior to providing access.

Physical devices and information must be protected.

- Store keys that can access organisation information in secure locations such as locked desk or cupboard
- Don't allow access to CCTV cameras to unauthorised individuals
- Store confidential papers in secure locations
- Store unattended physical devices in secure locations or take them with you

There is a Clear Desk Approach in place which must be followed.

Any physical documents that are sent externally via post must use recorded delivery if the document contains either confidential or private information.

# Encryption

All organisation devices must use device encryption where possible. All organisation confidential and private data must be encrypted in transfer and at rest (where the data is stored). Data in transfer should have TLS 1.3 or above in place and encryption at rest AES 256. All private or confidential information sent via email must be password protected and the password must be sent in a separate email or via SMS.

# Business Continuity and Disaster Recovery

Sheldon School has a business continuity and disaster recovery plan in place which identifies the organisation's critical assets; defines roles and responsibilities; and, documents recovery activities in the case of a disaster.

## Backups

Backups will be taken of organisations information systems to ensure that in the instance where the data is not available, the organisation is able to retrieve the backup data based on the Recovery Time Objective (RTO; how much down-time can be tolerated) and Recovery Point Objective (RPO; how often are backups taken and how much data would need to be re-entered) documented in the business continuity plan.

# Compliance

Sheldon's design, operation and management of information systems must be in accordance with all statutory, regulatory and contractual security requirements which includes:

- The Data Protection Act 2018
- The UK GDPR
- PCI DSS (where applicable)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)

Internal or/and external audits can be used to demonstrate compliance against chosen standards and best practice, including against internal policies and procedures.

Any breaches of this policy may be subject to the disciplinary process.