William College

Information Security Policy

Table of Contents

1. Introduction

William College manages, handles, and stores large volumes of data relating to learning, teaching, research, and professional and administrative activities. The purpose of this policy is to ensure that this data, and the IT resources that process it, are appropriately secured to mitigate risks that impact confidentiality, integrity, and availability. Failure to adequately secure data may result in financial and reputational damage, legal penalties, regulatory non-compliance, or disruption or denial of full or partial operations.

Information Security is an integral part of the College's culture. Therefore, it is the responsibility of all users of William College data to read, understand, and comply with this policy and associated information security policies and procedures.

It is the College'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
- **Accessibility** – information will be accessible to authorised users and processes when required

William College seeks to achieve robust information security and implement an Information Security Management System based on the international standard for information security management.

The College recognises the need for its students, staff, and visitors to have access to the data they require to carry out their work and studies. Information security helps protect against breaches of confidentiality, failures of data integrity, or interruptions to data availability, and ensures compliance with legal, regulatory, and contractual obligations.

2. Purpose and Scope

This policy ensures that information is appropriately secured to protect against the possible consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.
This policy applies to all information, regardless of the form or format, collectively termed "Information Assets," created or used in support of College activities. This includes:

- Any IT systems connected to the College's networks;
- Any IT systems provided by the College;
- Any communications sent to or from the College;
- Any data owned, controlled, or processed by the College, including data on systems external to the College network.
- All approved users of College data, including staff, students, contractors, suppliers, partners, and authorised external researchers.
- All locations from which College data is accessed, including home and off-site use.
- All equipment used to access the College's data.

3. Roles and Responsibilities

- The **Senior Leadership Team** is responsible for endorsing and supporting the implementation of this policy.
- The **IT Department** is responsible for maintaining secure infrastructure, monitoring compliance, and responding to security incidents.
- The **Data Protection Officer** (DPO) oversees compliance with data protection legislation and provides guidance on privacy matters.
- **All users**—including staff, students, and contractors— are responsible for adhering to this policy, completing relevant training, and reporting incidents or concerns promptly.

4. Policy Principles

4.1 Information Classification and Handling

All information held by the College must be classified based on its sensitivity. Information should be categorised as Public, Internal, Confidential, or Restricted, depending on the potential impact of its disclosure. Staff and students must handle information in accordance with its classification, using safeguards such as encryption, secure storage, and access control. Clear desk and screen policies, secure disposal of information, and secure file-sharing practices must be followed at all times.

4.2 Access Control

Access to information and systems must be strictly controlled and granted only to authorised individuals, based on their roles and responsibilities. The principle of least privilege must be applied to ensure users are granted only the access necessary to perform their duties. User accounts must be protected with strong passwords and, where possible, multi-factor authentication. Access rights must be reviewed regularly and removed promptly when no longer needed, such as when staff leave the College or change roles.

4.3 Use of Personal and Cloud-Based Devices

The use of personal devices (e.g., laptops, smartphones, tablets) for work-related activities is permitted only under the College's Bring Your Own Device (BYOD) Policy and must comply with defined security standards.
Users are responsible for ensuring that College data accessed on personal devices is stored securely and not shared or transmitted in an unauthorised manner.

4.4 Cloud Application and AI Systems

Any Cloud-based or AI-driven applications used for College-related work—whether accessed via personal or College devices—must be approved by IT Services before use. This includes, but is not limited to, tools for document creation, communication, storage, and AI processing.
AI systems, which often rely on large datasets containing personal information, require additional attention. William College acknowledges its ethical responsibility to conduct a proportionate and comprehensive assessment before the deployment of any AI systems that process personal data.

The College will retain its status as the data controller for any Cloud applications commissioned. Should a data breach occur in relation to these applications, the College is obligated to report the incident to the UK Information Commissioner's Office (ICO) in accordance with data protection regulations.

Before deploying any Cloud applications, thorough security and data protection assessments must be completed in line with the College's Third-party Applications Security Procedure. Key steps in this process include:

- The Department seeking to deploy applications or software must notify IT Services before engaging with suppliers.
- Where relevant, the Department must complete a Data Protection Risk Evaluation (DPRE) and/or a Data Protection Impact Assessment (DPIA), which will be reviewed by the College IT Department.
- The security assessment and DPIA must receive sign-off from both the IT Manager and the Data Protection Officer (DPO) prior to acquisition or download. Where applicable, these assessments must be integrated into the tender process.
- The security posture of the supplier must be reviewed at least annually to ensure continued compliance and security.

4.5 Data Protection and Privacy

All users of William College systems must comply with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Personal data must

be processed only with a clear legal basis and protected using appropriate technical and organisational measures, in line with the College's Data Protection Policy.
Staff and students must inform data subjects about how their data is used, stored, and shared. Breaches of data protection law may lead to disciplinary action, legal consequences, and reputational harm to the College.

4.6 Physical and environmental security

Information processing facilities must be located in secure areas, protected from unauthorised access, damage, or interference by physical security controls. Both internal and external controls must be implemented to prevent unauthorised access to sensitive assets, including those processed by third-party providers.

4.7 Communications security

The IT Department 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.

4.8 System and Network Security

The College implements robust technical controls to protect systems and networks, including firewalls, anti-virus software, intrusion detection systems, and regular vulnerability scanning. Systems must be configured securely and maintained in accordance with industry best practices. Software updates and patches must be applied promptly to protect against known vulnerabilities. The use of unsupported or outdated systems is prohibited unless specifically risk-assessed and approved with mitigating controls in place.

5. Information security incident management

All information security incidents or other suspected breaches of this policy must be reported immediately to the IT Department. For the escalation and reporting of data breaches including, but not limited to, data breaches that involve personal data, unauthorised access, loss or theft of devices, phishing attempts, or malware incidence, contact the Data Protection Officer, dpo@williamcollege.com.

Upon receipt, incidents will be assessed, categorised (e.g. high, medium, low severity). High-risk incidents, including those that may lead to a personal data breach, will be escalated to the Senior Leadership Team and, where required, reported to the Information Commissioner's Office (ICO) within 72 hours. A post-incident review will be undertaken to identify root causes and implement any necessary corrective actions.

6. Ethical Use and Oversight of Artificial Intelligence (AI)

The use of Artificial Intelligence (AI) technologies within William College are subject to clear ethical oversight to ensure fairness, transparency, and accountability. AI applications, particularly those involved in automated decision-making, profiling, or analysis of student and staff data, must not compromise individual rights, academic integrity, or institutional values. Any proposed deployment of AI tools must undergo a formal risk and ethics assessment led by the relevant department, with advice and oversight from the Data Protection Officer (DPO), IT Services, and senior academic governance structures.

Specific consideration is given to:

- **Bias and fairness**: Ensuring AI tools do not reinforce discriminatory practices or outcomes.
- **Transparency**: Providing clear explanations to users and subjects of AI-supported decisions.
- **Accountability**: Identifying responsible parties for decisions supported or made by AI.
- **Data minimisation and consent**: Ensuring only necessary data is used, with lawful processing grounds.

A Data Protection Impact Assessment (DPIA) is mandatory for any AI system that is likely to result in a high risk to individuals' rights and freedoms. William College maintains a register of approved AI systems in use, and their application are reviewed periodically to ensure alignment with evolving regulatory and ethical standards. All staff deploying or relying on AI systems are required to complete training in ethical data use and responsible digital innovation.

7. Awareness and Training

All users are provided with a range of awareness and training materials in relation to Information Security and relevant William College policies and procedures.

Awareness and training should take place on a regular basis, including during induction and then periodically afterwards.
Managers should discuss and share Information Security policies with Users at the earliest opportunity and offer support, help, and appropriate training where appropriate for the User's role.

8. Compliance

This policy and its implementation will be subject to internal monitoring and auditing, and the outcomes from these processes will inform and improve practices as part of a commitment to continuous improvement.
Any compromise of William College's systems and data could lead to possible financial penalties, recovery costs, reputation loss, and in severe cases, legal actions against the College. Therefore, it is essential that all users adhere to this policy and its requirements.

Any deliberate, malicious, intrusion to William College's systems by staff could result in disciplinary procedures or termination of contract. Non-compliance with this policy may also result in revocation of system access, or legal repercussions. William College reserves the right to monitor its systems to ensure adherence to this policy and to investigate any breaches. Serious or repeated violations may be escalated to senior leadership or reported to external authorities, such as the Information Commissioner's Office (ICO), when appropriate.

9. Review of the Policy

This Policy is reviewed annually by the Senior Leadership Team and may be triggered by legislative changes. Any amendments require the approval of our Board of Governors.

10. Related Internal Policies and External Reference Points

Internal Policies

- Data Protection Policy
- Privacy Notice
- Bring Your Own Device (BYOD) Policy
- Acceptable Use Policy
- Staff Disciplinary Policy
- Student Disciplinary Policy

External Reference Point:

- Equality Act 2010
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998

March 2025

Appendix A – DOs and DON'Ts

DOs

- Use a strong password: three random words in mixed case separated with punctuation.
- Change your password if you think it is compromised, and at least once a year.
- Back up your important data, e.g. to OneDrive and a USB disk.
- Tell someone (personal tutor, IT Service Desk) if you have any security concerns.
- Check your email regularly for security advice and alerts from IT Services.
- Watch out for phishing – online scammers pretending to be someone else.
- Be considerate of fellow students and staff when using IT systems and equipment.
- Read and follow the Data Protection Policy
- Respect copyright laws and software license agreements.
- Follow the rules and terms of use for third-party services provided by the College, such as Microsoft 365.

DON'Ts

- Never share your password or leave it written down where it can be found.
- Don't leave a logged-in computer unattended.
- Avoid downloading content from untrustworthy sources—they may contain malware or other harmful software.
- Do not bypass or disable security systems, such as antivirus software, or attempt to install unauthorized software, servers, or devices.
- Do not tamper with, move, or remove any College equipment without permission.
- Access only data you are authorised to use. Never view, modify, or delete someone else's information without their explicit consent.
- Information security is everyone's responsibility—it's not just an IT issue.
- Never access, create, store, or share content that is offensive, indecent, defamatory, extremist, or discriminatory based on race, gender, age, sexual orientation, marital status, disability, religion, or political views.
- Do not engage in any illegal activity or behaviour intended to defraud, harass, inconvenience, or harm others.
- Do not attempt to disrupt or damage the work or data of others or interfere with the College systems or networks.
- Do not use College systems for personal gain, or in ways that compete with or conflict with the College business or policies.

Appendix B – Definitions

Data includes but is not limited to any information accessed, stored, and/or processed on/by IT Resources, stored either digitally or hardcopy, in formats including, but not limited to text, graphics, images, sound, and video.

A **Data User** is any individual or system that uses data for undertaking the College's business.

Information is conveyed or represented by a particular arrangement or sequence of things, such as data.

Sensitive Data this is data from which individual/individuals are personally identifiable. It includes names, contact details (phone, address, email), initials, financial information. It can include any identifier of an individual, e.g. a job title can be personal data if it alongside other information that would allow someone to identify the individual), special category (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, generic data, biometric data, or data concerning health, a person's sex life, or a person's sexual orientation) and confidential (information which is confidential to the College for example for business reasons. This can include meeting papers and minutes, proposals for discussion, research and intellectual property, financial information like individual bank details or details of contracts. If you are unsure about the confidentiality of data, check with your line manager or the person/team which originated the data). This data must be protected from unauthorised access to safeguard its privacy and the security of individuals and the organisation.

Information Asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited efficiently. Information Assets have recognisable and manageable value, risk, content, and lifecycles.

Systems and Services are places or platforms where the College data can be entered, stored, or retrieved.

Information Security Risks to operations, assets, and individuals due to potential unauthorised access, use, disclosure, disruption, modification, or destruction of information and/or information systems. Risks that could cause the loss of confidentiality, integrity, and/or availability of William College data or IT Resources.

Integrity - to safeguard the accuracy and completeness of data.

Threat - an adversary or attacker that has the opportunity, capability, and intent to exploit a vulnerability to cause harm.

Vulnerability - a weakness, flaw, or misconfiguration in a system, process, or control that can be exploited by a threat. Can be both technical and human error.

Appendix C – Information Asset Ownership

To support effective data governance and ensure accountability for the protection of information, the College designates Information Asset Owners (IAOs) also referred to as Data Stewards for each significant dataset or system containing personal or sensitive data. IAOs are responsible for the classification, security, appropriate access controls, and retention of the information assets under their care. They are expected to ensure that data is processed lawfully, stored securely, and retained or disposed of in accordance with the College's Data Retention Schedule. IAOs are also responsible for identifying risks related to their assets and collaborating with the Data Protection Officer and IT Services to ensure compliance with relevant data protection legislation. A current register of designated IAOs will be maintained by the Data Protection Officer and reviewed annually.

Information Asset Owners (IAOs) – Roles and Responsibilities
Each Information Asset Owner (IAO) is accountable for the lifecycle management and protection of the data sets or systems under their control. IAOs are typically senior staff or heads of department who have operational authority over a particular set of information. Their responsibilities include, but are not limited to, the following:

1. Data Classification and Risk Assessment

- Ensure all data within their area of responsibility is classified appropriately (e.g. public, internal, confidential, or sensitive).
- Identify and assess risks associated with the data asset, including unauthorised access, loss, or breach.
- Work with the DPO to determine if a Data Protection Impact Assessment (DPIA) is required.

2. Access Control and Data Integrity

- Authorise user access to the asset and ensure access rights are based on the principle of least privilege.
- Review access permissions regularly to maintain data confidentiality and integrity.
- Ensure appropriate controls are in place to detect unauthorised access or misuse.

3. Legal and Regulatory Compliance

- Ensure data is processed in accordance with the UK GDPR, Data Protection Act 2018, and College policies.
- Ensure contracts with third-party processors include appropriate data protection clauses where relevant.
- Liaise with the DPO to ensure ongoing compliance and respond to any regulatory enquiries related to their data assets.

4. Data Retention and Disposal

- Apply and monitor compliance with the College's Data Retention Schedule for the asset.
- Ensure secure deletion or archiving of data at the end of its retention period.
- Document and report any deviations from standard retention practices to the DPO.

5. Security and Incident Management

- Ensure that appropriate technical and organisational measures are in place to protect the asset from loss, corruption, or unauthorised access.
- Promptly report any data breach or security incident involving the asset.
- Support post-incident reviews and implement recommendations for corrective action.

6. Training and Awareness

- Ensure that staff handling the data asset are aware of their responsibilities and have received appropriate information security and data protection training.
- Promote a culture of good data handling practice and risk awareness in their area of influence.

7. Documentation and Audit Readiness

- Maintain up-to-date documentation for the asset, including a description of its purpose, legal basis for processing, location, and security controls.
- Cooperate with internal and external audits related to the information asset.