William College

Acceptable Use of IT Services Policy

© William College. All rights reserved

Document Version Control	
Document Title:	Acceptable use of IT Services Policy
Version:	1
Reviewing Committee:	N/A
Approving Committee:	Senior Leadership and Management Team
Policy Lead:	IT Coordinator
Date of Last Review:	January 2026
Date of Approval:	May 2026
Date Effective from:	June 2026
Date of Next Review:	January 2028

© William College. All rights reserved

Table of Contents

1. Introduction ____ 3
2. General Use and Ownership ____ 3
3. Security and Proprietary Information ____ 4
4. Unacceptable Use ____ 4
   4.1 System and Network Use ____ 4
   4.2 Use of Email and Communication Channels ____ 5
   4.3 Internet Activity ____ 5
5. Enforcement ____ 6
6. Policy Review ____ 6
7. Related Policies and Documents ____ 6

© William College. All rights reserved

1. Introduction

This policy establishes the standards for the responsible use of William College's information resources by student, staff (employees), contractors, temporary workers, and external parties who have been granted access. Each role mentioned is responsible for complying with these standards.

2. General Use and Ownership

All forms of information assets, whether electronic or physical, are the property of William College and must be utilised exclusively for valid educational or business activities, in accordance with applicable policies and regulatory requirements such as data protection.

Access and usage of these resources are restricted to authorised individuals, and they must not be employed for improper or unethical purposes including, but not limited to, acts that contravene:

- **The Counter-Terrorism and Security Act 2015 (Prevent Duty):** Using the network to access, download, or disseminate extremist or terrorist material.
- **The Computer Misuse Act 1990:** Unauthorised access to computer material or impairing the operation of any computer.
- **The Equality Act 2010:** Harassment or discrimination against protected characteristics via the College's digital platforms.

Any event involving the compromise or destruction of these resources must be immediately communicated to the IT Coordinator.

William College maintains the right to oversee the use of its resources for reasons including, but not limited to:

- Confirming compliance with information protection policies.
- Fulfilling legal, contractual, and regulatory requirements.
- For ensuring the safety and well-being of its students, staff, and other parties.
- Other purposes deemed reasonable and appropriate by the institution, as compliant with applicable regulation and legislation.

Information created, stored, or processed within William College's systems, including official records and work-related materials, is subject to institutional information governance, security, and records management policies.

William College retains control over its systems and information for legitimate organisational purposes. Nothing in this policy should be understood as removing or limiting statutory rights individuals have over their personal data under applicable data protection law.

It is explicitly not allowed to access, reveal, duplicate, modify, reroute, delete, lose, exploit, or steal any data without proper authorisation. Users are advised to encrypt any sensitive or at-risk information to ensure its protection.

To uphold security and system integrity, authorised staff may inspect systems, devices, and network activity at any time. William College also reserves the right to perform routine checks of its infrastructure to ensure adherence to policies. Further details on how we protect our stakeholders at the network level are available in the Web Monitoring and Filtering Policy.

Internet and email services may be restricted should bandwidth issues or signs of misuse be detected.

© William College. All rights reserved

3. Security and Proprietary Information

Approved users are accountable for securing their login credentials. All desktop computers, laptops, and workstations must be safeguarded with password-protected screensavers that activate automatically, and users must lock or log off when leaving their devices unattended. Specific password guidelines are outlined in the Password Policy and user account standards defined in the Access Control Policy.

Any message sent from a corporate email account or identifying the sender as a William College staff member must include a disclaimer stating that the opinions expressed are personal, unless the communication is official.

All use of college systems involving personal data must comply with the Data Protection Act 2018 and UK GDPR. Users are reminded that they have a statutory duty to protect the confidentiality of student and staff data. Unauthorised disclosure, even accidentally via email misdirection, constitutes a data breach and may result in disciplinary action and personal liability under the Act.

Users should be vigilant when opening email attachments from unfamiliar sources, as these may contain malicious content. This is further addressed in the Anti-Malware Policy.

4. Unacceptable Use

The following behaviours are generally deemed inappropriate. Should a device interfere with operational services, system administrators may remove its network access.

No individual is allowed to perform unlawful actions—whether under domestic or international law—while using William College-owned equipment. The examples provided are illustrative and not exhaustive.

4.1 System and Network Use

- Sharing login credentials or permitting others to use your personal account —including household members during remote work— is not allowed. Each user is accountable for all actions taken under their account.
- Using organisational devices or systems to access, send, or request material that breaches sexual harassment laws or fosters a hostile workplace is unacceptable.
- Installing or distributing software without valid licensing, including pirated or unauthorised programs, is strictly not allowed.
- Reproducing or sharing copyrighted content—such as music, software, images, or excerpts from books and magazines—without proper authorisation is forbidden.
- Revealing internal data, such as user or client lists, to outside parties without approval is not permitted.
- Trying to compromise system security or interfere with network operations—such as accessing restricted data or logging into unauthorised accounts or servers—is a major breach, unless such access is part of official responsibilities.

In accordance with the Counter-Terrorism and Security Act 2015, the College has a statutory duty to prevent people from being drawn into terrorism. The use of College IT equipment or networks to access, store, or disseminate material that glorifies, promotes, or encourages terrorism is strictly prohibited and will be reported to the relevant authorities.

Notwithstanding the College's commitment to academic freedom under the Higher Education (Freedom of Speech) Act 2023, this policy does not protect the expression of views that constitute unlawful speech, including harassment under the Equality Act 2010 or incitement to hatred.

© William College. All rights reserved

Any concern related to safeguarding will be referred to the Designated Safeguarding Lead as per the Safeguarding and Prevent Policy.

4.2 Use of Email and Communication Channels

- Sending mass or unsolicited emails, including spam or promotional messages, to recipients who have not opted in is not allowed.
- Using email to intimidate others—through offensive language, excessive messaging, or large attachments—is prohibited.
- Email must not be used to pose as someone else or to elicit responses under false pretences with the aim of misleading or harassing.
- William College email accounts must not be used to distribute defamatory remarks or personal opinions about colleagues, vendors, partners, or clients.
- Email messages should be sent only to relevant recipients to minimise unnecessary data exposure.
- Creating or forwarding chain messages, hoaxes, or similar schemes is forbidden.
- Attachments sent externally via email must be assessed to determine if encryption or other security measures are needed.
- Users must be cautious when opening attachments from unknown or unexpected sources, even if they appear to be from familiar contacts. Suspicious messages should be reported to the IT Coordinator and must not be shared or forwarded.
- Any email containing virus alerts or hoaxes must be reported to the IT Coordinator and must not be redistributed.
- William College email addresses should only be used on websites for official business purposes. Personal use or registration on non-business platforms is not allowed.
- Automatically forwarding emails to external accounts is not permitted unless there is a justified and approved business need.
- Manipulating email headers or impersonating another user's identity without permission is strictly disallowed.
- Email must not be used to make purchases on behalf of the organisation without prior authorisation and in line with procurement procedures.
- Using organisational email accounts for personal purchases or financial transactions is not allowed.

4.3 Internet Activity

- William College email addresses, websites, and user credentials must be used exclusively for sanctioned business-related communication.
- Downloading programmes or running scripts from the internet is only allowed when it complies with organisational guidelines and has received IT approval.
- All files obtained online must undergo antivirus malware scanning before being opened.
- Users are prohibited from uploading or sharing any organisational materials on public platforms without prior written consent.
- VPN access to the organisation's internal network is limited to individuals who have received direct authorisation from their supervisor.
- William College retains the right to track internet, email, and messaging activity for purposes of security, compliance, and network oversight as per the Web Filtering & Monitoring Policy. Traffic may be restricted when necessary.
- Any confirmed or suspected cybersecurity incidents must be reported to the IT Coordinator without delay.
- Users should refrain from downloading or streaming large media files—such as videos, audio, or high-resolution images—that consume excessive bandwidth and are unrelated to work tasks.
- William College disclaims responsibility for any offensive, inappropriate, or explicit material encountered online. Users access online content at their own discretion and must refrain from unlawful actions such as hacking or data theft. Any such behaviour will be escalated to law enforcement authorities.
- Users are not permitted to circumvent or disregard the William College's malware protection protocols.

© William College. All rights reserved

- Limited personal browsing is permitted as long as it does not disrupt professional duties or degrade system performance.
- Disrupting normal network functionality or obstructing others from accessing the network is strictly forbidden. Accessing, altering, or using another individual's files or data without consent is also not allowed.
- Access to the internet is provided in accordance with the Jisc (Janet) Acceptable Use Policy. Users must adhere to this policy's prohibitions on material that is defamatory, obscene, or infringes on third-party rights. The College is legally required to investigate and act upon complaints regarding copyright infringement (Copyright, Designs and Patents Act 1988), including the use of peer-to-peer file sharing software on the College network.

5. Enforcement

All individuals are required to comply with the organisation's defined information security standards and procedures. While routine or systematic monitoring is not conducted, the organisation reserves the right to investigate suspected misuse.

Breaches may lead to disciplinary action, which could include dismissal from employment, termination of contract, or cancellation of agreement depending on the seriousness of the offence. For students, repeated or severe breaches of this policy might lead to disciplinary action under the Student Disciplinary Policy and Procedures. Additionally, where a breach involves a suspected criminal offence (including but not limited to breaches of the Computer Misuse Act 1990, Terrorism Act 2006, or Data Protection Act 2018), the College may refer the matter to the Police, the Information Commission (IC)[1], or the Office for Students (OfS) as required by its statutory duties.

6. Policy Review

This Policy is reviewed and approved every eighteen months, or earlier if there are changes in partners' policies or the regulatory framework by the Senior Leadership Team.

7. Related Policies and Documents

- Password Management Policy
- Web Filtering and Monitoring Policy
- Staff Disciplinary Procedures
- Anti-Malware Policy
- Safeguarding and Prevent Policy
- Student Disciplinary Policy and Procedures
- Data Protection Policy

[1] The new name of the Information Commissioner's Office as a result of new legislation (Data (Use and Access) Act 2025 (DUAA)).

© William College. All rights reserved