

IT Acceptable Use Policy

1. Scope and Purpose

- 1.1. The Loughborough College Group is committed to the secure and appropriate use of its digital and communications systems.
- 1.2. All users, staff, students, applicants, contractors, and partners are expected to comply with the Group's information security policies and uphold the integrity and confidentiality of its data and systems. These apply to Loughborough College Group, its colleges, and its subsidiaries. References to the Group or College refer to all parts of the group.
- 1.3. This policy outlines expectations, legal responsibilities, and prohibited activities related to the use of technology.
- 1.4. Failure to comply may result in disciplinary action and/or legal proceedings.

2. Policy Statement

- 2.1. College IT resources are provided to support academic, administrative, and operational activities. Users are expected to act responsibly, ethically, and lawfully by using IT resources for authorised purposes only. Any activity that is illegal, disruptive, harassing, threatening, or impedes others' work or learning is strictly prohibited.

3. Impact Assessments

- 3.1. This policy/procedure has undergone an impact assessment process during review to ensure that any foreseeable risks and implications have been appropriately considered.
- 3.2. Equal Opportunities: The policy has been reviewed to uphold principles of equality and non-discrimination in accordance with equal opportunities legislation, ensuring fair treatment for all individuals.
- 3.3. Data Protection: All personal data processing activities governed by this policy have been assessed for risk and are fully compliant with current data protection laws. Privacy-by-design has been embedded as a core approach, with safeguards implemented to protect data subjects.
- 3.4. Safeguarding, Health & Safety, and Environmental Sustainability: Relevant aspects of safeguarding, health and safety, and environmental sustainability have been impact assessed to support a secure, inclusive, and responsible working and learning environments for all.

Name:	IT Acceptable Use Policy	Owner:	IT
Document Reference:	IT-PCG-003	Last Review:	August 2025
Version:	1.0	Next Review:	August 2026

*This document is the property of the Loughborough College Group.
Any reproduction, even partial, is prohibited without prior written agreement.
Document "uncontrolled" when printed.*



4. Policy

4.1. All users of The Loughborough College Group's IT systems are subject to routine monitoring and data logging to ensure compliance with this policy and with the Group's overarching Information Security and Monitoring Policies.

4.2. General Acceptable Use

4.2.1. All users must log in to systems using their college-issued credentials and may not share their username, password, or access tokens with others. Users are required to take responsibility for the protection of their credentials and must not attempt to access any systems or data for which they do not have explicit authorisation.

4.2.2. The use of another individual's credentials or access rights is strictly prohibited. Attempts to bypass system security or access control mechanisms, or to exploit vulnerabilities for unauthorised purposes, are violations of this policy and may result in disciplinary or legal action.

4.3. Classification and Handling of Information

4.3.1. All users are responsible for ensuring that information classified as sensitive or confidential is appropriately protected. This includes the secure storage, transmission and disposal of both digital and physical records.

4.3.2. Users must take steps to ensure that sensitive data is not accidentally disclosed, including verifying recipient email addresses before transmission and using encryption for transmitting classified or personal data over unsecured networks.

4.3.3. Printed materials must be handled securely, protected from unauthorised access, and destroyed per information disposal guidelines when no longer required.


4.3.4. When working in public or shared environments, users must remain vigilant to the possibility of being overlooked and take appropriate precautions.

4.4. Device Security and Remote Working

4.4.1. Users must not leave computers or mobile devices unattended while logged in, particularly in shared or public areas. Any mobile or portable device that stores or accesses Group data must be secured at all times, particularly when used outside the office. This includes, but is not limited to, ensuring that devices are encrypted and not left in exposed locations, such as unattended vehicles. College devices are encrypted automatically, but personal phones will not be.

Name:	IT Acceptable Use Policy	Owner:	IT
Document Reference:	IT-PCG-003	Last Review:	August 2025
Version:	1.0	Next Review:	August 2026

*This document is the property of the Loughborough College Group.
Any reproduction, even partial, is prohibited without prior written agreement.
Document "uncontrolled" when printed.*

- 
- 4.4.2. Removal of IT equipment or data from The Loughborough College Group premises requires prior authorisation. All computer media, including USB drives and laptops, must be safeguarded in transit and use, with data encrypted where applicable.

4.5. Multi-Factor Authentication (MFA)

- 4.5.1. Multi-Factor Authentication (MFA) is a mandatory requirement for accessing Group systems that contain sensitive, financial, or personal data. MFA enhances login security by requiring a second method of verification (e.g., a mobile authentication app, hardware token, or SMS code).
- 4.5.2. All staff and students are required to maintain the confidentiality and security of their second authentication factor and must report any loss or compromise to IT Services immediately.
- 4.5.3. MFA is enforced on, but not limited to, the following systems:
- Microsoft 365 services (including Outlook, Teams, OneDrive)
 - Remote Desktop/VDI, VPN, and cloud-hosted platforms

4.6. Malware and System Protection


- 4.6.1. Users are prohibited from introducing or attempting to introduce viruses, malware, or other forms of malicious software into the network, including pirated software.
- 4.6.2. Altering or disabling antivirus software, firewall settings, or Group-installed security configurations is not permitted.
- 4.6.3. Only authorised IT Services personnel are permitted to perform software installations or changes to system configurations.

4.7. Data Breach, Incident Reporting and Exit Procedure

- 4.7.1. Users must immediately report any suspected information security incidents, breaches, or weaknesses to their line manager or the IT Helpdesk.
- 4.7.2. Before leaving the Group at the end of employment, users must ensure that important information, access credentials, and files are returned or transferred to their line manager or another designated staff member to avoid disruption or data loss.

Name:	IT Acceptable Use Policy	Owner:	IT
Document Reference:	IT-PCG-003	Last Review:	August 2025
Version:	1.0	Next Review:	August 2026

*This document is the property of the Loughborough College Group.
Any reproduction, even partial, is prohibited without prior written agreement.
Document “uncontrolled” when printed.*

- 
- 4.7.3. All College devices must be returned to IT or HR, not their line manager, at the end of their employment. Failure to do so may result in the staff member being responsible for the cost of a replacement device.

4.8. Legal and Regulatory Compliance

- 4.8.1. Users are required to adhere to all relevant legal, statutory and contractual obligations, including but not limited to:

- UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Prevent Duty Guidance
- JISC Acceptable Use Policy

- 4.8.2. Compliance with this policy is a condition of employment or enrolment. Breaches may result in disciplinary measures and, where applicable, legal prosecution.

4.9. Responsibilities

- 4.9.1. It is the responsibility of everyone to ensure they understand and comply with this Acceptable Use Policy and all associated policies. Failure to do so may result in the revocation of access rights and further disciplinary action.

- 4.9.2. Questions regarding this policy should be directed to the line manager or the IT Services department.

5. Location and Access

- 5.1. This document can be found here:

- The Loughborough College Group's Website
- The Loughborough College Group's SharePoint

6. Linked Policies and Procedures

- 6.1. You may wish to view the following policies:

- Information Security Policy
- Monitoring Policy

Name:	IT Acceptable Use Policy	Owner:	IT
Document Reference:	IT-PCG-003	Last Review:	August 2025
Version:	1.0	Next Review:	August 2026

*This document is the property of the Loughborough College Group.
Any reproduction, even partial, is prohibited without prior written agreement.
Document "uncontrolled" when printed.*



- Mobile Device Policy
- Network Security Policy
- Cloud Computing Policy
- Electronic Messaging Policy
- Access Control Policy
- Anti-Malware Policy
- Privacy and Personal Data Protection Policy
- Information Security Incident Response Procedure

7. Change Log

Date	Version	Details of Change	Reviewer	Reviewer Title

Name:	IT Acceptable Use Policy	Owner:	IT
Document Reference:	IT-PCG-003	Last Review:	August 2025
Version:	1.0	Next Review:	August 2026

*This document is the property of the Loughborough College Group.
Any reproduction, even partial, is prohibited without prior written agreement.
Document “uncontrolled” when printed.*