IT Acceptable Use Policy

1. Scope and Purpose

The Loughborough College Group is committed to the secure and appropriate use of its digital and communications systems.

This policy applies to all staff, students, governors, applicants, contractors, agency workers, volunteers, partners and visitors who access the Group's information, systems, networks or devices. It applies whether access is from Group premises, remotely, through a personal device or through a third-party service. References to the Group or College include all colleges and subsidiaries within The Loughborough College Group.

This policy outlines expectations, legal responsibilities, and prohibited activities related to the use of technology.

Failure to comply may result in access being restricted or withdrawn, action under the relevant staff or student disciplinary procedure, recovery of losses and, where appropriate, referral to the police or another regulatory or statutory body.

2. Procedure Statement

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

This document has been assessed for its impact on equal opportunities and will be informed by the aim to eliminate all forms of discrimination in all strands of the equal opportunities' legislation.

This document has been assessed for potential risk on data subjects due to the processing of personally identifiable information. All processing has been reviewed and is in line with all current Data protection laws and appropriate safeguards implemented to ensure that the policy has privacy by design as its underlying approach.

Name:	IT Acceptable Use Policy	Owner:	IT & Digital
Approved by:	Executive Lead	Applicable to:	All
Reference:	IT-PCG-003	Last Review:	Apr 2026
Version:	1.1	Next Review:	Aug 2027

This document has been impact assessed where appropriate for Safeguarding, Health and Safety and Sustainability Factors to ensure that all potential risks are identified and mitigated, and that the policy supports a safe, inclusive, and environmentally responsible learning and working environment.

4. Procedure

Use of the Group's systems, networks and devices may be logged, filtered and monitored for security, safeguarding, service management, legal and regulatory purposes. Monitoring will be undertaken in accordance with the Group's Monitoring Policy, privacy notices and applicable law, and will be necessary, proportionate and limited to authorised personnel.

General Acceptable Use

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.

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.

Classification and Handling of Information

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.

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.

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

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

Device Security and Remote Working

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.

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

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) must be used for Group accounts and services wherever it is provided or required by IT Services. Users must follow the approved sign-in process and must never approve an unexpected authentication request or disclose a one-time code.

Users must protect their authentication device, token and recovery information and report any loss, compromise or unexpected prompt to IT Services immediately.

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
- Any other externally accessible College services

Reasonable Personal Use

Limited and occasional personal use of Group systems is permitted where it is lawful, reasonable, does not interfere with work or learning, does not create material cost or risk, and does not breach this or another Group policy. Personal use may be restricted or withdrawn at any time.
Users must not use a Group email address, identity, brand or resource to imply Group endorsement of a personal view, outside business, political campaign or commercial activity unless formally authorised.

Users should not store personal files or communications on Group systems. The Group does not guarantee the privacy, availability or recovery of personal content held on its systems.

Email, Messaging, Internet and Social Media

Email, messaging, collaboration platforms and internet access must be used professionally and with the same care as other formal communications. Users must check recipients, attachments, links and the sensitivity of information before sending, sharing or posting.

Users must not create, access, store or distribute material that is unlawful, fraudulent, defamatory, discriminatory, threatening, harassing, extremist, obscene or otherwise likely to cause harm. A limited exception may apply where access is necessary for an authorised, lawful and appropriately supervised teaching, research, safeguarding or investigative purpose.

Users must not send unsolicited bulk messages, chain messages or unauthorised marketing; impersonate another person; conceal their identity for improper purposes; or make statements on behalf of the Group without authority.

Suspected phishing or malicious messages must be reported using the approved reporting method. Users must not open suspicious links or attachments, reply to the sender or forward the content to others except as directed by IT Services.

Approved Systems, Cloud Services and Artificial Intelligence

Group information must only be created, stored, processed or shared using systems and cloud services approved by the Group. Users must not bypass procurement, security, data protection or records-management controls by using unapproved applications, personal accounts or consumer file-sharing services.

Confidential, commercially sensitive, personal or special-category data must not be entered into public or unapproved artificial intelligence services. Users remain responsible for checking AI-generated content for accuracy, bias, confidentiality, copyright and suitability, and must follow the Group's guidance on academic integrity and the responsible use of AI.

Automated decision-making, recording or transcription tools must not be used where they could affect an individual or capture personal data unless the activity has been authorised and any required data protection assessment, consent or notification has been completed.

Personal Devices, Removable Media and Software

Personal devices may access Group services only where permitted and must use a supported operating system, current security updates, screen locking and appropriate device protection. The Group may block or remove access from any device that presents a security risk.

Group information must not be downloaded to, or permanently stored on, a personal device unless explicitly authorised and protected by approved security controls. Users must take particular care where a device is shared with family members or others.

Unknown or USB storage devices will be denied access to college systems. Lost or stolen devices or media must be reported immediately.

Software, browser extensions and applications may only be installed or used where they are licensed, supported and approved by IT Services. Users must not use pirated software or circumvent licence, security or management controls.

Prohibited Technical Activity

Unless specifically authorised as part of a user's role, users must not scan, probe, intercept or monitor networks; test or exploit vulnerabilities; obtain elevated privileges; access another person's files or communications; connect unauthorised equipment; run cryptocurrency mining, peer-to-peer sharing or anonymising services; or deliberately disrupt, overload or damage any service.

Users must not delete, alter, conceal or destroy Group records outside an authorised retention and disposal process, nor deliberately evade filtering, monitoring, audit, backup, security or access controls.

Malware and System Protection

Users are prohibited from introducing or attempting to introduce viruses, malware, or other forms of malicious software into the network, including pirated software.

Altering or disabling antivirus software, firewall settings, or Group-installed security configurations is not permitted. Only authorised IT Services staff are permitted to perform software installations or changes to system configurations.

Data Breach, Incident Reporting and Exit Procedure

Users must immediately report suspected phishing, malware, unauthorised access, accidental disclosure, loss or theft of equipment, misdirected communications, security weaknesses or any other information security incident to the IT Helpdesk. Safeguarding concerns must also be reported through the Group's safeguarding procedure. Users must not investigate an incident themselves, delete relevant evidence or delay reporting because all details are not yet known.

Before leaving the Group or changing role, users must transfer business records and ownership of relevant files to an authorised colleague. Passwords and personal authentication factors must not be shared; access will be reassigned or reset through the approved IT process with HR approval.

All Group equipment, security tokens, removable media and other information assets must be returned to IT Services or HR, as directed, when employment, study, placement or other authorised access ends. The Group may seek recovery of equipment or costs where items are not returned.

Safeguarding and Online Safety

Technology must be used in a way that supports the safety and wellbeing of children, young people and adults at risk. Staff must maintain professional boundaries, use approved channels for communication with students and never use personal accounts or unapproved services for such contact.

Users must not attempt to bypass the Group's filtering or monitoring controls. Any online content, contact or behaviour that creates a safeguarding concern must be reported immediately in accordance with the Safeguarding Policy and procedure.

Legal and Regulatory Compliance

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) and Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Equality Act 2010
- Human Rights Act 1998
- Investigatory Powers Act 2016 and applicable communications legislation
- Prevent duty guidance and current statutory safeguarding guidance
- Jisc Janet Acceptable Use Policy

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

Responsibilities

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

5. Location and Access to Procedure

This document can be found on:

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

6. Linked Policies and Procedures

- Information Security Policy
- Monitoring Policy
- Mobile Device Policy
- Network Security Policy
- Cloud Computing Policy
- Electronic Messaging Policy
- Access Control Policy
- Anti-Malware Policy
- Safeguarding Policy
- Artificial Intelligence Policy or Guidance
- Staff and Student Disciplinary Procedures

7. Change log

Date	Version	Details of Change	Reviewer	Reviewer Title
August 2026	1.1	Policy reviewed and updated for current security, safeguarding, cloud and AI requirements. • Wider coverage of users, devices, remote access and third-party services. • Clearer consequences for non-compliance. • Updated monitoring, MFA, phishing and incident-reporting requirements. • New rules covering personal use, communications, cloud services, AI and social media. • Stronger controls for personal devices, removable media, software and prohibited technical activity. • Additional safeguarding, online-safety and leaver requirements. • Updated legislation, linked policies, review dates and change log.	Chris Manton	Executive Director IT & Transformational Change Programmes