HUGHES HALL
UNIVERSITY OF CAMBRIDGE

Acceptable Use of IT Policy

Executive summary: Government legislation, University and College regulations and protocols serve as the basis of this policy, which applies to every member of the Hughes Hall community who has access to and uses the College's IT facilities, resources, programmes and tools. This policy defines the role of IT support, expectations and instructions for users, and clear boundaries between acceptable and unacceptable use. Actions arising from misuse, inappropriate or criminal conduct are also outlined.

Table of contents

1. Policy Purpose 2
2. Scope 2
3. Definitions 2
4. Responsibilities 2
5. Policy Statement 3
   5.1 Key principles of acceptable use: 3
   5.2 Data protection and information management: 3
   5.3 Security: 4
   5.4 Artificial Intelligence (AI) and Generative AI: 4
   5.5 Social media use: 5
   5.6 Bring your own Device (BYOD): 5
   5.7 Overseas working: 5
   5.8 Unacceptable use of IT Systems: 5
   5.9 Privacy and Monitoring: 6
   5.10 Breaches and Disciplinary Procedures: 7
   5.11 Staff Usage: 7
6. Associated Documents 8
7. Appendices 9
8. Implementation / Communication / Training 9

Policy owner: Bursar	Version number: 1.0
Effective date: 24/06/2026	Date of review: June 2027
Approving Body: Council	Location: website

1. Policy Purpose

1.1 This policy establishes the framework for the acceptable, secure, and ethical use of the College's Information Technology (IT) systems, services, equipment and digital resources. Its purpose is to promote a safe and productive digital environment for all members of the community and to ensure the security of data and systems from damage and threats, whether internal, external, deliberate or accidental.

1.2 The College provides IT systems and equipment to support teaching, learning, research, personal educational development, activities that directly or indirectly support the operations and business of the College and any other lawful activity that furthers the College's charitable objectives. Access is conditional upon compliance with this policy. Users are expected to understand and comply with this policy.

2. Scope

2.1 Hughes Hall, or the 'College', is the institution to which this Acceptable Use of IT Policy applies. It comprises all staff, students, researchers, senior members, visitors, contractors, alumni or authorised external users. It encompasses their use of College IT systems and equipment, taking into account all physical sites and should be read in conjunction with the associated policy documents set out in Section 6. Due to variation in circumstances between students and other members of the College some aspects of this policy are not applicable to student members. Such clauses are clearly indicated.

2.2 This policy ensures that every user of the College's IT Systems understands their responsibilities when using College resources and how to use the systems in an acceptable way, and helps them to make appropriate decisions about their online and network usage.

2.3 All Users should be aware of and adhere to this policy. Contravention of these rules or non-compliance could lead to loss of access to IT facilities and disciplinary action. Users who are unsure about any aspect of this Acceptable Use of IT Policy or the use of Hughes Hall IT systems should seek clarification by contacting the Hughes Hall IT Department.

2.4 Whilst this Policy primarily governs the use of College IT systems, networks and equipment, conduct undertaken outside College systems (including on personal devices or networks) may be considered under relevant College policies and procedures where it is unlawful and/or it poses a safeguarding, legal or reputational risk to the College or its community.

3. Definitions

Users	All staff, students, researchers, senior members, visitors, contractors, alumni or an external user authorised to access and use College systems.
Equipment	All College-owned devices (computers, mobile devices, telecommunications devices, servers), or personal devices when connected to the College networks e.g. via Eduroam or VPNs, and physical infrastructure.
Systems	Email, Virtual Learning Environments (VLE), cloud storage, administrative databases, internet access and digital infrastructure.

4. Responsibilities

4.1 The College operates under strict legal obligations. All users must comply with UK legislation and relevant EU regulations (outlined in Section 6). Failure to comply may result in personal criminal prosecution or civil liability.

4.2 This Policy will be implemented fairly and transparently at all times and should be read in conjunction with the College's other policies outlined in Section 6.

4.3 Every user must comply with the regulations and expectations of this Acceptable Use of IT Policy and must not engage in unacceptable uses, including those outlined in Section 5.8. The College reserves the right to prohibit the use of networks due to policy violations.

4.4 All security/cyber-security incidents and any technical problems including those pertaining to the IT Systems should be immediately reported to IT Support at help@hugheshall.on.spiceworks.com.

4.5 Incidents involving confidential College or personal data, or loss of data/information must be reported without delay to compliance@hughes.cam.ac.uk who will notify the College Data Protection Lead.

4.6 The IT Manager and Assistant Bursar, working alongside the leadership team, are responsible for overseeing and ensuring implementation of this Policy, as well as its regular review and update.

4.7 All IT Systems are to be installed, maintained, serviced, repaired and upgraded by IT Support or by such third parties authorised by IT. Users must not attempt to rectify problems on their own.

4.8 Hughes Hall accepts no responsibility for the integrity of any program or data stored on its machines.

4.9 All users must complete mandatory annual cybersecurity training delivered by the University Information Service and regularly complete Boxphish training modules, which users receive by email.

5. Policy Statement

5.1 Key principles of acceptable use:

5.1.1 Users are expected to exercise good judgement, and to treat others with respect in all electronic and virtual communications. Staff and senior members should demonstrate professionalism in their communications. All members must handle IT equipment with care, keeping all systems and programs up to date by running updates when directed.

5.1.2 Users must not connect or power unauthorised equipment (e.g., Wi-Fi routers, digital currency mining equipment) through the network or attempt to bypass security controls (e.g., using proxies to evade web filtering).

5.1.3 The Hughes Hall IT network and systems are linked to the University of Cambridge's network, therefore all usage of the College's computing facilities is also subject to the University's policies issued by UIS (University Information Services), available at: Information Security Policies | IT Help and Support (cam.ac.uk).

5.2 Data protection and information management:

5.2.1 Data stored on College IT Systems will be available only to users with a legitimate need for access and must be used/accessed appropriately and responsibly.

5.2.2 All College data must be stored on approved databases or servers (e.g. OneDrive/SharePoint), not on local desktops or unencrypted USB drives. All student personal data stored on IT Systems are to be managed securely in compliance with the Data Protection Policy, however, staff should not store personal files on College databases.

5.2.3 Confidential or student/staff personal data transfer should be restricted to OneDrive and SharePoint/Teams. In the context of a work environment, no confidential or personal data should be transferred to a personal or external device without the permission of the Bursar or Compliance Manager and may only be transferred in cases where the user is contracted to work on behalf of the College and has agreed to comply with the Data Protection Policy and GDPR.

5.2.4 Any suspected data breach (e.g. accidental email to wrong recipient, lost laptop) must be reported to the IT Helpdesk and compliance@hughes.cam.ac.uk immediately.

5.2.5 Users should be vigilant regarding any potential security threats including but not limited to: manipulation to divulge confidential information or secure system access, phishing for account details or a customised attack on a specific member or members of the College (via questionable emails and attachments etc.).

5.3 Security:

5.3.1 All remote access to College systems and servers must be via an approved VPN connection or other approved remote access means.

5.3.2 No hardware, software or platform shall be downloaded without review by the IT Manager and where personal data will be processed, the Compliance Manager. Software installations must be approved by the IT Manager.

5.3.3 All IT Systems will be protected with suitable anti-virus, firewall, and other appropriate internet security software. Any virus detected must be reported immediately to IT Support.

5.3.4 IT Support will take necessary action to remedy any problems related to viruses. In limited circumstances this may involve the temporary removal of the affected computer or device.

5.3.5 Users should not open ANY links in e-mails, unless they can validate the sender, nor should they open attachments from unknown parties. Contact the Helpdesk if you are unsure.

5.3.6 Users should never enter their Office 365 username or password into any e-mail, text message, or provide the details to any caller or to any other source other than College-provided computers or software that requires it, without first checking with IT Support that the request is legitimate, even if the contact comes from a seemingly known or trusted source.

5.3.7 If doubt arises over the legitimacy of an e-mail, users should raise a ticket with the IT Help Desk immediately to seek advice.

5.3.8 Any user who does not follow this threat protection guidance and is found to have provided their Office 365 details to an unauthorised source will be subject to the College's formal disciplinary procedures, up to and including gross misconduct.

5.3.9 Other than laptops and meeting room desktop PCs, users will not have access to other IT Systems (including, but not limited to, servers, networking equipment, and network infrastructure).

5.3.10 All printing and photocopying is recorded against a user-ID and is the responsibility of the person to whom the ID is registered, unless that ID has previously been reported as compromised.

5.3.11 The loss or theft of equipment which could be used to access College systems must be reported immediately to the IT Department.

5.3.12 Devices containing College data or which have access to its systems shall be encrypted, protected with a passcode and/or secure, random password and must be multi-factor authentication (MFA) enabled.

5.3.13 Users must never share or record their password and if a password is comprised it must be changed immediately (forgotten passwords can be reported to IT and a temporary one issued).

5.3.14 Hardware must be locked and secured when left unattended at any location other than private homes. Unattended devices on College premises must be locked to prevent unauthorised access.

5.3.15 It is forbidden to create a wireless hotspot or share an internet connection.

5.3.16 Users are responsible for all activity conducted under their login and should never allow others to use/access their account. Likewise, it is forbidden for users to use IP addresses, user-IDs and associated computer resources not allocated specifically to them.

5.4 Artificial Intelligence (AI) and Generative AI:

5.4.1 The College encourages the responsible use of AI to enhance learning, research, and productivity. However, AI tools must be used as **supportive assistants**, not replacements for critical thinking or original work.

5.4.2 Users must **never** enter the following into public/open generative AI tools as public AI models may use such input to train their systems, making that data retrievable by others outside the College:

5.4.2.1 Personal data; that is data that can lead to an individual being identified, directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

5.4.2.2 Confidential research data or unpublished intellectual property.

5.4.2.3 Sensitive commercial or administrative information.

5.4.3 Users are solely responsible for verifying and critically evaluating all AI-generated content for accuracy and bias (including considering the source data) in any output they use for teaching, assignments or work tasks.

5.4.4 Students submitting work generated entirely or partially by AI as their own without acknowledgement is **plagiarism**. The University's guidelines on AI and plagiarism can be found here. Its guidance on the use of generative AI is here. The University also offers guidelines on the use of AI in Assessments

5.4.5 Students must clearly cite how AI was used (e.g., "used for brainstorming," "used for code debugging") in their submission statement.

5.5 Social media use:

5.5.1 For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. Users, whether acting in an official or personal capacity should not:

5.5.1.1 Post offensive or inappropriate content, including but not limited to defamatory and/or knowingly false material and/or unauthorised material about the College and its members, on any social networking or other online publishing format.

5.5.1.2 Harass, threaten or intimidate others.

5.5.1.3 **I**n the case of users apart from students, promote commercial activities and content linking to the College without prior approval from the College.

5.5.2 Users can state a preference not to appear in Social Media updates, by registering their request at comms@hughes.cam.ac.uk and compliance@hughes.cam.ac.uk.

5.6 Bring your own Device (BYOD):

5.6.1 BYOD relates to staff's personal devices (including but not limited to laptops and mobile phones) used to access any College information asset and/or network service. Limited exceptions to the policy may occur due to variations in devices and platforms.

5.6.2 All personal devices used for College business must be appropriately protected, kept up-to-date and disposed of securely.

5.6.3 The Acceptable Use of IT Policy must be followed when using a personal device for College work or permission to use this device may be revoked.

5.6.4 Users who wish to access College systems or data using a personally owned device must register that device with the College's IT Support Team before use. Registration may require providing details of the device, agreeing to relevant security requirements, and allowing the College to apply necessary security controls. The College reserves the right to restrict or revoke access from any unregistered or non-compliant device.

5.7 Overseas working:

5.7.1 Members of Hughes Hall working outside of the UK for operational, academic or personal reasons on a short-term basis must comply with this policy in its entirety.

5.7.2 The production, collection and/or processing of business-related information in the course of work abroad remains the property of the College. This includes such information stored on third-party and social networking websites.

5.7.3 Staff and any senior members who have a Hughes Hall account and access to College systems and who intend to access these systems or College data while travelling outside the United Kingdom must notify and register their travel with IT Support in advance of departure. These users must provide the destination country or countries, travel dates, and the device or devices that will be used to access College resources. IT may apply additional security controls or restrict access where necessary to protect College systems and information.

5.8 Unacceptable use of IT Systems:

The following activities are strictly prohibited and internet access may be monitored to ensure they do not occur (disciplinary action in line with student or staff procedures may also be taken):

5.8.1 Harassment & Abuse: Creating or transmitting material (including emails) that is offensive, obscene, false, defamatory, derogatory, threatening, discriminatory in that the context is a personal attack, sexist or racist, or might be considered as harassment including material which breaches the college's Equality, Inclusion and Diversity Policy, Anti-harassment and Anti-bullying Policies).

5.8.2 Extremism: Accessing or promoting material that incites violence, radicalisation, or terrorism (unless pre-authorised for specific academic research via the Ethics Committee).

5.8.2.1 Under the Prevent Duty, encouragement of terrorism and inviting support for proscribed terrorist organisations are criminal offences. Users are not permitted to create, download, store, transmit or display material that promotes or incites hatred, terrorism or hate crimes.

5.8.2.2 Any students with concerns about terrorism or hatred material encountered by themselves or others should contact their College Tutor.

5.8.3 Copyright Infringement: Using peer-to-peer (P2P) file-sharing networks to download and pirate illegal music, movies, or software; accessing copyrighted information in a way that violates the copyright.

5.8.4 Commercial Activity: Library resources are intended for academic use and must not be used for commercial purposes. Users may not engage College IT resources or systems for private business, with the intent to earn money or for cryptocurrency mining. In addition, users (not including students) must not use Hughes Hall IT systems for political campaigning.

5.8.5 Malicious Activity: Creating or distributing viruses, malware, perpetrating any form of fraud against other users or hacking into unauthorised areas. Hacking is a dismissible offence for staff.

5.8.6 Breach of confidentiality: Revealing confidential information about the College in a personal online posting, upload or transmission to external parties - including financial information and information relating to College members, business plans, policies, staff and/or internal discussions.

5.8.7 Other inappropriate distribution activities include but are not limited to: undertaking deliberate activities that waste staff effort or network resources; transmitting unsolicited commercial or advertising material or consuming excessive bandwidth causing degradation to the service. Users, apart from students who may access systems for personal use, may not broadcast unsolicited personal views on social, political, religious or other non-business-related matters.

5.9 Privacy and Monitoring:

5.9.1 The College respects the privacy of its users. However, in order to protect its IT systems, users, data and wider legitimate interests, the College may monitor the use of its IT systems, accounts, networks and devices where it is lawful, necessary and proportionate to do so. The College may also review publicly available online content where this is relevant to a suspected serious breach of College rules, a risk to users or systems, or a legal or safeguarding concern.

5.9.2. Monitoring may be carried out for purposes including:

- maintaining the security and integrity of the College's IT systems;
- preventing, detecting, investigating or responding to suspected breaches of this policy, other College rules or applicable law;
- safeguarding users and protecting the rights, property and reputation of the College and others; and
- meeting the College's legal and regulatory obligations.

5.9.3 Any monitoring will be targeted and limited to what is reasonably required in the circumstances. The College will not carry out monitoring that is excessive or unjustifiably intrusive.

5.9.4 Information obtained through lawful monitoring may be used in connection with investigations and may be referred to the appropriate College procedure, including student disciplinary, staff disciplinary or other relevant processes, as applicable.

5.9.5 Access logs and other relevant system records may be retained for 12 months for security, auditing and investigative purposes in accordance with the College's data protection requirements and retention arrangements.

5.10 Breaches and Disciplinary Procedures:

5.10.1 Any person believed to be in breach of Hughes Hall or the University of Cambridge's rules and policies is liable to have their User-ID, or other access to the College network, summarily suspended and to be reported to the appropriate College Officer.

5.10.2 This College Officer may at their discretion impose further appropriate disciplinary action, including financial penalty and/or the removal of all rights to use the Hughes Hall IT facilities under the relevant disciplinary policy/procedure.

5.10.3 Legal Action: where the College reasonably believe that use of its electronic communication systems constitutes a criminal offence, (e.g., child sexual abuse material, hacking) the College may contact the relevant law enforcement authorities without notifying the user and will cooperate in any subsequent investigation or action.

5.10.4 Refusal to engage with the Hughes Hall and/or the University of Cambridge's Acceptable IT Use Policy and associated processes may, in the most serious cases, result in the initiation of the relevant disciplinary procedure.

5.11 Staff Usage:

5.11.1 In addition to compliance with the rest of the policy in its entirety, as well as the Staff handbook, members of staff must also adhere to the requirements stipulated in this section. Misuse of IT systems, equipment and inappropriate use of personal devices may result in disciplinary action.

5.11.2 Use of equipment:

5.11.2.1 The College's equipment is only to be used for college business. All of its equipment used on and off college premises should be used responsibly and with care to avoid damage and disruption, including from drink spillage.

5.11.2.2 Faults, losses or damage must be reported to the appropriate contact immediately and will be subject to an investigation by management. Abuse or negligent use of equipment will be investigated under the disciplinary procedure and any losses or damages attributable to negligence, misuse or by any other contributory fault on the staff member's part will render them liable to pay for a replacement or repair in full or in part.

5.11.2.3 On termination of contract of employment staff members must return to the College all of its property in their possession including data and IT equipment.

5.11.2.4 Limited use of Hughes Hall's network and IT facilities for personal purposes other than work during break times e.g. access to the internet, is permitted although the use of personal devices and conducting of personal business during work hours should be kept to a minimum. Such use must not interfere with work, must be legal, and must be strictly in line with this policy.

5.11.3 Security:

5.11.3.1 Staff members should not delete, destroy or modify existing systems, programs, information or data, which could have the effect of harming the College or exposing it to risk.

5.11.3.2 No information belonging to the College, especially member details, should be taken off the premises e.g. on laptops or USB sticks without adhering to proper GDPR guidelines.

5.11.3.3 Creating, viewing, accessing, transmitting or downloading any content which is likely to create any criminal or civil liability for that staff member or the college will amount to gross misconduct.

5.11.4 Social Media and Professional Conduct:

5.11.4.1 Staff participation in social media activity must adhere to the standards of conduct expected by the College in maintaining honesty, integrity, confidentiality, professionalism, respect, responsibility and trust**.**

5.11.4.2 Staff should avoid bringing the College's name into disrepute or embarrassment in any online presence and communication and ensure that colleague and client confidentiality or rights to privacy are not compromised.

5.11.4.3 Staff must not visit internet sites that contain obscene, hateful, pornographic, gambling, gaming or otherwise illegal material.

5.11.4.4 Hughes Hall has dedicated social media accounts set up to communicate information and employees must only use these with authorisation and for purposes approved by the Head of Communications.

5.11.4.5 The College reserves the right to monitor employees' use of social media on the College's equipment. The College considers that valid reasons for checking a staff member's internet usage include suspicions that the staff member has been using social media when they should be working or acted in a way that is in breach of the rules set out in this policy. Monitoring of social media will consist of checking the sites visited, the amount of time spent on them, and the content the staff member contributed.

5.11.5 Email use

5.11.5.1 Staff should not: use college email for private correspondence (including messages relating to non-work events or activities) or unnecessary communication with colleagues, or gamble. In addition, they must not agree to terms or enter into contractual commitments without the appropriate authority, (offers or contracts transmitted via e-mail are as legally binding on the College as those sent on paper), send messages from another staff member's computer or under an assumed name or send confidential messages that are known not to be secure.

5.11.5.2 All College business and communications must be carried out via the Hughes Hall email system, using @hughes.cam.ac.uk addresses and the necessary steps must be taken to protect confidentiality.

5.11.5.5 Please be aware that inappropriate use of email is potentially gross misconduct and could result in dismissal.

5.11.6 Monitoring:

5.11.6.1 The College may monitor staff use of its IT systems, including computers, telephones, and email, where it is necessary and proportionate to achieve legitimate business purposes or to fulfil legal obligations as an employer. Any such monitoring will be targeted and limited to what is strictly required to ensure compliance with College policies and investigate alleged wrongdoing, or maintain business continuity (such as retrieving messages lost due to computer failure or during unexpected staff absence). The College reserves the right to monitor internet usage for security purposes (including pages visited and searches made) using automated screening via Microsoft Defender which flags security risks to be reviewed by the IT Team. This process does not include automated processing of personal data. Any incidental monitoring of permitted personal use (as defined in clause 5.11.2.4) will be kept to an absolute minimum. For full details on the lawful bases for processing, data retention periods, and your rights, please refer to the Data Protection Statement for Staff.

5.11.6.2 The information gathered through monitoring may be shared internally, if the College has reasonable grounds to believe that there has been a breach of the rules set out in this policy. It may be shared with a staff member's line manager, managers in their department and IT staff if necessary. Information gathered will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted. Information obtained through monitoring will not be disclosed to third parties other than our external HR consultancy and/or legal advisers, (who comply with our data protection policies), unless the College is under a duty to report matters to a regulatory authority or to a law enforcement agency.

6. Associated Documents

6.1 This Policy will be implemented fairly and transparently at all times and should be read in conjunction with the College's other policies:

6.1.1 Data Protection Policy.

6.1.2 (*Student only*) Disciplinary Policy (Students) including the Rules of Behaviour.
6.1.3 (*Employee only*) Staff Handbook.
6.1.4 *(Senior members)* Statutes and Ordinances.
6.1.5 Social Media Policy

6.2 University policies

6.2.1 Information Security Policies | IT Help and Support (cam.ac.uk).
6.2.2 Antivirus software | IT Help and Support (cam.ac.uk).

6.3 UK Legislation and Guidance

6.3.1 Computer Misuse Act 1990: It is a criminal offense to access any program or data without authorisation, or to modify data (e.g., hacking, introducing viruses) without permission.

6.3.2 UK General Data Protection Regulation 2021 (UK GDPR) and Data Protection Act 2018 : Users must process personal data lawfully, transparently, and securely.

6.3.3 Copyright, Designs and Patents Act 1988: Users must respect intellectual property rights. Downloading pirated software or media is strictly prohibited.

6.3.4 Counter-Terrorism and Security Act 2015 and Prevent Duty Guidance 2023: The College has a duty to prevent people from being drawn into terrorism. IT systems must not be used to access or disseminate extremist material.

6.3.5 Equality Act 2010: IT systems must not be used to harass, discriminate against, or victimise individuals based on protected characteristics.

6.3.6 Investigatory Powers Act 2016: Governs the College's right to intercept and monitor communications under specific circumstances.

6.4 EU and Global Data Protection Regulations

6.4.1 Any transmission of personal data between the College, EU or global partners is managed through agreed processes that comply with the relevant country's data protection legislation.

7. Appendices

N/A

8. Implementation / Communication / Training