Document Reference Number	**UoG/ILS/IS 005**
Title	Policy for Acceptable Use of Email, Internet, Software and Cloud Facilities
Owning Department	Information and Library Services
Version	3.0
Approved Date	06/11/2025
Approving Body	IT Management Board (IM)
Review Date	05/11/2026
Classification	Non-sensitive

Version Control

Version	Last Modified	Last Modified By	Document Changes
3.0	06/11/2025	Principal Strategy and Information Security Officer	Annual review. Reworded for clarity.
2.8	09/10/2024	Head of Information Security and Compliance	Added version control. Updated document titles.

Policy for Acceptable Use of Email, Internet, Software and Cloud Facilities

1.0 Introduction

1.1 University IT facilities must be used in a responsible manner that aligns with applicable legal and ethical standards, as well as professional conduct expectations. Academic staff should also refer to the overarching principles outlined in the Code of Good Practice Regarding the Professional Rights and Responsibilities of Academic Staff.

2.0 Purpose and Scope

2.1 This policy, along with its supplementary guidelines, defines the responsibilities and acceptable practices for using the university's email, internet, software, and cloud services. Its aim is to ensure these resources are accessed only by authorised individuals and used appropriately.

2.2 This policy applies to all individuals who access the university's email, internet, software, and cloud services, regardless of whether they are on campus or working remotely.

2.3 The university reserves the right to access, monitor, or review any information stored within its IT systems and infrastructure.

3.0 ISO 27001 Reference

3.1 This policy complies with the university's Information Security Strategy and draws upon the ISO 27002 Code of Practice.

4.0 Use of Cloud Platforms

4.1 The university provides tools and guidance to support the secure and appropriate use of third-party cloud services. All users are required to follow established procedures to protect university data stored or processed on these platforms.

4.2 Access to university cloud facilities must be carried out on secure networks, using devices with up-to-date security controls.

4.3 Where feasible, cloud services must be integrated with the university's single sign on solution. This simplifies logon, provides multi factor authentication and supports centralised account management.

4.4 Multi-factor authentication is mandatory for all university staff accessing cloud services.

4.5 Users must keep their authentication credentials confidential. Multi factor authentication should be disabled on devices that are no longer in use.

4.6 Collaboration and data sharing on cloud platforms must be conducted in a manner that ensures appropriate security and complies with university policies and procedures.

4.7 Users must obtain the necessary authorisations for specific activities, such as requesting guest access to Office 365 Teams, approval of privacy impact assessments for personal data usage, or using university data on non-standard cloud collaboration platforms.

4.8 Access to university cloud services on mobile devices must comply with the university's Policy for Mobile and Remote Working.

5.0 Use of Email

5.1 All information held by the university, including email content, may be subject to disclosure under applicable Data Protection Legislation.

5.2 Users must ensure email communications comply with Data Protection Legislation and follow the Procedure for Data Classification, Labelling and Handling. This includes, but is not limited to:

- Sharing personal information without the data subject's consent.
- Retaining personal information longer than necessary.
- Sending personal information to another country.

5.3 Emails are considered official university records and a legal form of written communication. Users should exercise discretion and avoid sharing content that may be deemed inappropriate or unprofessional.

5.4 Only university provided email systems may be used to transmit university data. Use of external email services (e.g. Gmail, personal Outlook accounts via web or mobile apps) is prohibited due to data security risks.

5.5 Automatic forwarding of university emails to personal accounts (e.g. Hotmail, Gmail, Yahoo) or unaffiliated third parties is not permitted. Exceptions must be reviewed and approved by the Executive Director and Chief Information Officer or a nominee.

5.6 Caution must be exercised when emailing personal data. Any email containing personal information may be subject to disclosure under Data Protection Legislation. This includes factual content as well as opinions. Emails containing confidential or sensitive information may also be disclosed under the Freedom of Information Act 2000.

5.7 University email must not be used to transmit content that is illegal, obscene, defamatory, or associated with harassment, impersonation, discrimination, violence, extremist ideologies, or any activity that could result in legal or disciplinary action. Inappropriate emails received from university staff, students, or external parties should be reported to a line manager or academic supervisor. All email communications must reflect professional standards and avoid offensive language.

5.8 Documents shared via email must uphold the university's brand integrity and reputation.

5.9 Users may not impose confidentiality restrictions on emails stored within the university's systems. Emails may be disclosed under legal or regulatory frameworks, including the Freedom of Information Act, Data Protection Legislation, legal proceedings, or internal investigations. Users are responsible for all activity associated with their email and network accounts and must prevent unauthorised access.

5.10 Occasional personal use of university email is permitted, provided it is reasonable, does not interfere with university operations, and does not compromise system security or the university's reputation.

5.11 University email credentials (username and password) must not be used to register accounts on external platforms such as social media, online retailers, or personal cloud services.

5.12 Any third-party systems used by the university that may require university email or username for account registration must be authorised by Information and Library Services. University passwords must never be used on such systems or sites.

5.13 University email should not be used as permanent document storage or archiving. Use of email client archiving is not permitted.

5.14 Bulk communications to staff and students must be distributed through channels approved by Internal Communications. Unsolicited mass emails are prohibited.

5.15 Email messages in the Deleted Items folder will be automatically removed after 30 days**.**

5.16 Users should regularly clean their inboxes by permanently deleting junk and obsolete messages. Emails requiring long-term retention should be saved to approved storage areas and removed from the inbox.

5.17 All outbound university emails must include the standard corporate disclaimer. No other disclaimers are permitted.

5.18 All information processing resources, including email systems, are provided for legitimate use. The university reserves the right to monitor and access email accounts without prior notice to ensure business continuity during prolonged absences or to investigate suspected misuse or retrieve critical information.

5.19 Any email activity that could compromise the university's IT systems must be reported immediately to the IT Service Desk.

6.0 Use of Internet

6.1 Internet access is encouraged for employees and students when it supports their work or studies. The university reserves the right to monitor internet usage across all devices connected to its network, including personally owned equipment.

6.2 Reasonable personal use is permitted subject to the following:

6.2.1 Users must not post or upload personal information to the university's website without the data subject's consent and must follow approved procedures for web authoring and editing.

6.2.2 Users must not engage in online activities that could bring the university into disrepute or create or transmit material that may be defamatory or incur liability on the part of the university or adversely impact the university's reputation.

6.2.3 Accessing, viewing, or downloading illegal or inappropriate content is strictly prohibited. This includes, but is not limited to, pornography, obscene material, race-hate material, content promoting violence, criminal activity, extremist ideologies, terrorist groups, cults, gambling, illegal drugs, or any material intended to harass or offend others. Use of the internet for criminal purposes such as piracy, fraud, terrorism, or the sale of illegal items is also forbidden.

6.2.4 Users must not intentionally introduce any form of computer virus or attempt to gain unauthorised access to restricted areas of the university's network.

6.2.5 Personal internet use must not degrade system performance or increase demand on university resources such as bandwidth, storage, or processing capacity.

6.2.6 Downloading commercial software or copyrighted materials is prohibited unless covered by a valid license or agreement.

6.2.7 The internet must not be used for personal financial gain.

6.2.8 Personal browsing (e.g. online banking, shopping, general surfing) must be limited, reasonable and must not interfere with work or study responsibilities.

6.3 In the event of inadvertent access to a site serving or suspected of serving malicious content, immediately contact the IT Service Desk.

6.4 Use of social media platforms including, but not limited to, Facebook, Instagram, TikTok, LinkedIn, YouTube, X and WhatsApp, is permitted provided it is reasonable, proportionate and does not interfere with work or studies. Non-work or study related access should be limited to breaks or non-working hours unless there is a specific academic or professional need. Please refer to the university's Social Media Policies for staff and students.

7.0 Use of Software

7.1 The university is committed to meeting all legal and contractual obligations related to software licensing.

7.2 No software product or application subject to licensing or usage conditions shall be installed or made available on any university computer or IT system, for which a prior license has not been procured or properly acquired or renewed.

7.3 Users must comply with all terms and conditions outlined in the licensing agreements or contracts under which software is provided by the university, including any published usage restrictions.

7.4 All applicable Conditions of Use must be followed once software has been made available for use.

7.5 Where any such license restricts the use of the software to a specific number of users, those limits must be strictly observed.

7.6 Users are responsible for ensuring compliance with licensing requirements, regardless of whether the software product or application is purchased outright, leased, renewed, hosted via a third-party or provided as freeware.

8.0 Legitimate Access to Prohibited Material

8.1 In certain cases, academic or professional activities may necessitate access to materials that are otherwise restricted under this policy. Such access must be discussed and approved in advance with the appropriate authority, namely, a line manager for staff or an academic supervisor for students. Where access is required for legitimate, properly supervised research purposes, approval must be obtained from the university's Research Ethics Committee prior to engaging with the material.

9.0 Monitoring

9.1 The university reserves the right to access and examine its IT systems and the data stored within them at any time and without prior notice, where deemed necessary beyond routine business operations. Such access supports compliance with university policies and legal obligations, facilitates internal investigations, and aids in the effective management of information systems.

9.2 Network traffic is monitored and filtered to ensure the university meets its regulatory responsibilities.

9.3 In accordance with Section 26 of the Counter-Terrorism and Security Act 2015 and the UK Governments Prevent Strategy, the university is required to take measures to prevent individuals from being drawn into terrorism.

9.3.1 As part of this duty, the university will implement reasonable monitoring of network activity to identify and respond to content deemed unacceptable under the Prevent strategy. This includes material related to terrorism, extremism or content of a particularly hateful nature.

9.3.2 The university will monitor traffic and internet activity within its own network.

9.3.3 Where appropriate, and in line with legal requirements, the university will report relevant findings to the appropriate authorities.

10.0 Penalties for Improper Use

10.1 While the university encourages responsible and constructive dialogue, any actions or communications that bring the university into disrepute may be considered misconduct. Such cases will be subject to investigation under the university's disciplinary procedures.

11.0 Charging

11.1 Misuse of university IT facilities may result in disciplinary action, which may include the recovery of any associated costs incurred during the proceedings.

11.2 Users found to be in breach of this policy, or related regulations, may have their access to university IT services restricted or revoked.

11.3 Where applicable, breaches of the law will be reported to the civil authorities.

12.0 Policy Compliance

12.1 Access to the university's on-premise and cloud-based IT facilities is restricted to authorised users only. All users are required to comply with this policy. Misuse of access privileges is strictly prohibited and should be reported to the IT Service Desk.

12.2 The necessary steps to verify compliance to this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

12.3 Failure to adhere to this policy may be addressed under the university's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the information security policies.

12.4 Upon termination of employment or expiration of authorised access for students, guests, or third parties, access to IT facilities will be revoked in accordance with the User Account Management and Access Control Policy. Any exceptions to this process must be formally approved as outlined in that policy.

13.0 Exception to policy

13.1 Any exception to this policy must be approved by the Executive Director and Chief Information Officer or a nominee.

14.0 Policy Review and Maintenance

This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

15.0 Related Policies, Processes and Standards

- University Information Security Policies
- Information Compliance Policies
- Counterterrorism and Security Act 2015 (Prevent Duty Guidance)