| | |
|---|---|
| **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 | 2.8 |
| Approved Date | 09/10/2024 |
| Approving Body | IT Management Board (IM) |
| Review Date | 08/10/2025 |
| Classification | Public – Non-sensitive |

Version Control

| Version | Last Modified | Last Modified By | Document Changes |
|---|---|---|---|
| 2.8 | 09/10/2024 | Atif Siddique | Added version control. Updated document titles. |
| | | | |
| | | | |

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

## 1.0 Introduction

1.1 The university's IT facilities must be used responsibly and comply with the ethical and legal obligations that apply to them, as well as professional expectations (academic staff members are reminded of the overarching expectations set out in the Code of Good Practice Regarding the Professional Rights and Responsibilities of Academic Staff).

## 2.0 Purpose and Scope

2.1 The purpose of this policy and supplementary guidelines is to set out the responsibilities and practice for using the email, internet, software and cloud facilities to ensure these facilities are used only by authorised individuals and appropriately.

2.2 This policy applies to all users (on or off-premise) of the university's email, internet, software and cloud facilities.

2.3 Any information stored within the university's IT facilities may be subject to scrutiny by the university.

## 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 continues to provide tools and guidelines to ensure appropriate and secure use of the third-party cloud services it utilises. All users are to follow the relevant procedures and guidelines to safeguard the university's data stored and processed on these platforms.

4.2 Access to university cloud facilities must be carried out on secure networks and the devices used for accessing these facilities must have up-to-date security controls.

4.3 Where possible, access to 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 Access to cloud services used by university staff must require multi-factor authentication.

4.5 Users must ensure that their authentication details to the university's cloud and other IT facilities are kept secret. Multi factor authentication on devices should be disabled when the devices are no longer used.

4.6 Collaboration and information sharing on these platforms must be carried out in ways that provide the most appropriate security for these activities in compliance with the university's policies and procedures.

4.7 Relevant authorisations must be obtained where required e.g. Requests for Office 365 Teams Guest access, approval of privacy impact assessments for collection and use of personal data, and use of university data on other collaboration cloud platforms that are not part of the standard enterprise offerings.

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

## 5.0 Use of Email

5.1 Any information which the university holds is potentially disclosable to a requester under any of the applicable Data Protection Legislation. This includes email.

5.2 When using email, users are to ensure they are not breaching any Data Protection Legislation and are acting in accordance with the Procedure for Data Classification, Labelling and Handling. This could include but is not limited to:

- Passing on personal information without consent from the data owner.
- Keeping personal information longer than necessary.
- Sending personal information to another country.

5.3 Emails form part of the official records of the university and are treated as a legal form of written communication. Care should be taken to avoid communicating information that may be regarded as unsuitable or unacceptable.

5.4 Only university provided email systems must be used when transmitting university data via email. Use of any external email service provider such as Google Mail or Outlook via means of the email provider's website or phone app is not permitted as this presents a risk to university data.

5.5 Automatic email forwarding to personal email accounts such as Hotmail, Google Mail, and Yahoo or non-university affiliated partners is prohibited. Required exemptions will be reviewed and agreed in advance by the Executive Director and Chief Information Officer or a nominee.

5.6 Email should be used carefully when transmitting personal data. Any email containing personal information about an individual may be liable to disclosure to that individual under the Data Protection Legislation. This includes comments and opinions, as well as factual information. This must be considered when writing emails, and when keeping them. Emails that do not contain personal information but contain other information that may be classified as confidential or sensitive may be liable to disclosure under the Freedom of Information Act 2000.

5.7 University email should not be used to communicate any content that is pornographic, illegal, obscene or defamatory, or in connection with activities (including impersonation, bullying or harassing, malicious, discriminatory, offensive or abusive comments about ethnicity or nationality, gender, disability, age, sexual orientation, appearance, religious belief and practice, political belief or social background, to promote acts of violence, or to promote extremist ideologies and activities associated with terrorist groups) which could result in criminal or civil actions against an individual and/or the university. Employees or students who receive emails with such content from other employees or students of the university or external parties should report the matter to their line manager or academic supervisor. University email should be used professionally and must not contain any phrases or remarks that may be offensive directly or indirectly.

5.8 Documents sent via email must not compromise the integrity of the university's brand and reputation.

5.9 The university does not recognise any rights of email users to impose restrictions on the disclosure of emails held in the university's system. Emails may be disclosed under the Freedom of Information Act or Data Protection Legislation, as part of legal proceedings (e.g. tribunals) or disciplinary investigation proceedings. Users are responsible for all actions relating to their network and email accounts and should therefore make every effort to ensure no other person has access to their accounts.

5.10 Ad hoc use of university email for personal purposes is permitted but must be reasonable and not disrupt the university's wider IT systems (e.g. spreading of any form of virus or malware), interfere with work or studies of other colleagues and students or harm the university's reputation, bring it into disrepute, or incur liability on the part of the university.

5.11 University email and user login details (username and password) must not be used to register an account on any system or site not owned or used by the university e.g. social media networks, online stores, and personal cloud services.

5.12 Any third-party systems used by the university that may require the use of university email or username to register user accounts for that system 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 facility. Use of email client archiving is not permitted.

5.14 Bulk Messaging: All messages to staff and students should be communicated by methods approved by Internal Communications. Unsolicited emails must not be sent to staff and students.

5.15 Email messages in the **Deleted Items Folder will be deleted automatically after 30 days.**

5.16 Inboxes should be cleaned up periodically to remove unwanted emails (junk and obsolete) permanently. Where email messages need to be retained for long periods, these should be saved on the appropriate network drive and the emails deleted from the inbox.

5.17 The university attaches a standard corporate disclaimer to outbound email. No other disclaimer must be used.

5.18 All information processing resources of the university, including email, are provided for legitimate use. Without prior notice, the university maintains the right to monitor and access all systems including email accounts to allow the continuity of business where the account owner is on a prolonged absence, or to retrieve messages communicated through the email where there is a reasonable cause to believe an email account is being used inappropriately or holds information that may be critical to an investigation.

5.19 Where a user's activity on the email system could compromise the university's IT systems, this must be reported immediately to the IT Service Desk.

## 6.0 Use of Internet

6.1 Use of the Internet by employees and students is encouraged where such use is consistent with their work or studies, and the university reserves the right to monitor the use of the internet on all computer systems including personally owned devices connected to the university's network.

6.2 Reasonable personal use is permissible subject to the following:

6.2.1 Users must not post or upload personal information onto the university's website without the consent of Data Subjects, and/or without following correct procedures for web authoring and editing.

6.2.2 Users must not participate in any online activities that are likely to bring the university into disrepute, create or transmit material that may be defamatory or incur liability on the part of the university, or adversely impact on the reputation of the university.

6.2.3 Users must not visit, view, or download any material which contains illegal or inappropriate content. This includes, but is not limited to, pornography, obscene matter, race-hate material, violence condoning messages, criminal skills, materials which promote extremist ideologies and activities associated with terrorist groups, cults, gambling, illegal drugs, or to send offensive or harassing materials to other users. Users must not use the internet for illegal or criminal activities, such as but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal items including drugs.

6.2.4 Users must not knowingly introduce any form of computer virus to the university's computer network or seek to gain or hack into restricted network areas.

6.2.5 Personal use of the internet must not cause an increase in service required, e.g. storage, capacity, and speed or reduce system performance.

6.2.6 Users must not download commercial software or any copyrighted materials belonging to third parties unless such downloads are covered or permitted under a commercial agreement or other such licenses.

6.2.7 Users must not use the internet for personal financial gain.

6.2.8 Use of the internet for personal purposes (e.g. online banking, shopping, information surfing) must be limited, reasonable and not distract from work.

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

6.4 Use of social networking sites such as, but not limited to, Facebook, LinkedIn, YouTube, Twitter, WhatsApp, Flickr, Myspace, etc., is allowable so long as it is reasonable, proportionate and does not interfere with work or studies. Access other than for legitimate business, academic or study purposes, should be confined to breaks, lunch or other non-work or study periods unless there is a specific work or study-related need. Please refer to the university's Social Media Policies for staff and students.

## 7.0 Use of Software

7.1 The university must ensure it can satisfy its legal and contractual obligations with regards to the licensing of software products or applications.

7.2 No software product or application, to which license conditions or Conditions of Use pertain, shall be 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 All users of software products or applications must ensure that, where applicable, all requirements of the agreements or contracts under which licensed software is made available by the university are adhered to and they must comply with any published usage restrictions.

7.4 The Conditions of Use of any such product or application shall be adhered to subsequent to the software being made available for use.

7.5 Where any such license restricts the use of the software to a limited number of users, such limits will be strictly adhered to.

7.6 All users must remain conscious of their responsibilities for ensuring licensing requirements are satisfied regardless of whether the software product or application is purchased outright, leased, renewed, hosted via a third-party or freeware[1].

## 8.0 Legitimate Access to Prohibited Material

8.1 There may be circumstances where work or studies require access to, or use of materials prohibited under this policy. If so, this should be discussed with the line manager (for staff) or academic supervisor (for students) in advance. In the case of properly supervised or legitimate research purposes, it is acceptable to access such materials following approval by the university's Research Ethics Committee.

## 9.0 Monitoring

9.1 In cases where the university deems it necessary to examine data beyond that of its normal business activity, the university reserves the right at any time and without prior notice to examine any systems and to inspect and review all data held in these systems. This examination will help to ensure compliance with policies and the law. It will facilitate internal investigations and assist in the management of information systems.

9.2 The university monitors and filters its network traffic to fulfil its regulatory obligations.

9.3 The university has an obligation to have due regard to the need to prevent people from being drawn into terrorism, as specified under Section 26 of the Counter-Terrorism and Security Act 2015 and the Governments Prevent Strategy.

9.3.1 As part of this effort, the university will take reasonable measures to monitor network activity to detect usage which is considered unacceptable under the Prevent strategy. Unacceptable usage in this scenario is material that is deemed to be related to terrorism, extremism or of a particularly hateful nature.

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

9.3.3 Where necessary, the university will report any relevant findings to the appropriate authorities as required by legislation.

[1] Software product and application vendors are increasingly changing their licensing models, which has the potential to incur significant financial cost to the university. For example, the new licensing model for some Oracle products now allow the vendor to charge the license cost for the total number of employees, even if there is only a single instance of non-compliance with the licensing conditions.

## 10.0 Penalties for Improper Use

10.1 The university has no wish to stifle responsible discussion about itself. However, instances where the university is brought into disrepute may constitute misconduct and if so, will be investigated under the university's disciplinary procedures.

## 11.0 Charging

11.1 The relevant disciplinary proceedings will apply including associated costs thereof, for misuse of IT facilities.

11.2 Withdrawal of IT facilities: Users in breach of this policy and related regulations may have their access to university IT facilities restricted or withdrawn.

11.3 Breaches of the law: Where appropriate, breaches of the law will be reported to the civil authorities.

## 12.0 Policy Compliance

12.1 University on-premise and cloud IT facilities are provided only to those who have been authorised to use these facilities. All users of these facilities must comply with this policy. Any misuse of access privileges is 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 At the end of staff employment or the permitted access period to these facilities for students, guests and other third parties (please refer to the User Account Management and Access Control Policy), access will be terminated. Any exception to disable access will go through the approval process as stated in the User Account Management and Access Control 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)