University of Lancashire

Email and Instant Messaging Policy

Applicable from September 2025 to Present

Version	Issue Date	Revision description	Author	Approved by & date	Next review date
1	September 2023		Claire Miller	Academic Quality and Standards Committee: May 2023	May 2024
2	September 2024	Change to definition of 'Users' in section A to clarify that Users are any individuals with a University-provided email address, not just those with a University email address. Change to section G to clarify that 'LIS' also includes any third party service providers engaged by LIS. Section H - new subheadings for clarity. Section H - new sub-section about malicious emails referring to the use of phishing simulations and to introduce a requirement on Users to follow LIS guidance designed to help users identify malicious emails. Section K - removal of a bullet point for accuracy	Claire Miller	Academic Quality and Standards Committee: May 2024	May 2025
3	September 2025	Change of policy title from Email Use Policy to Email and Instant Messaging Policy, to make it clear from the title that the policy refers to more than email and includes other electronic messages. Definitions within the policy have not changed as they already incorporated these types of messages. Section F – added restrictions on use of University email address and network password for non-University accounts and systems, for security purposes to make it explicit that University email accounts and network passwords must not		Academic Quality and Standards Committee: July 2025	May 2026

		be used to register for third party accounts. Section H – changes to strengthen restrictions on using non-University email addresses for University business, and addition of a new section about using unapproved messaging tools. For security and data protection reasons, to make it clearer that non-University accounts must not be used for University business. Section K – removal of JANET AUP from the list of policies. This is a policy that the University complies with, rather than individual users, so is not appropriate to include.			

Purpose of policy	This policy sets out what is considered to be acceptable and unacceptable use of the University's email system. Breaches of the rules in this policy may result in the imposition of sanctions set out in the Rules for the Use of IT facilities and/or formal disciplinary action being taken pursuant to the Regulations for the Conduct of Students.
Internal services involved in authorship & implementation	Legal and Governance
Related University regulations, policies & guidance	Regulations for the Conduct of Students Rules for the use of the University's IT facilities IT Security Policy
Policy lead	Claire Miller
Equality impact assessment date	Equality Impact Assessment (EIA)
Data protection impact assessment date	Information Governance - Home

Contents

A Introduction and definitions

Email and other forms of electronic messaging are important and much-used services within the University. Email and messaging services are provided by the University to support its primary purposes of education and research and their associated functions. When used properly, email and other electronic messaging supports efficient and effective business processes.

This policy sets out what is considered to be acceptable and unacceptable use of the University's Email System. It informs users about the management of the Email System, the expectations of privacy users of the Email System should have and helps users and the University avoid legal risks which can arise as a result of using email and other types of electronic messaging. Further guidance on the appropriate and effective use of emails is available in Appendix A.

- *Email System* means the email system itself and any other IT products, technology and facilities which the University makes available for the purposes of sending or receiving electronic messages and attachments, instant messages (e.g. via Teams) and other similar communications including those sent via University-managed social media accounts and within collaborative platforms such as Teams and SharePoint.
- *Email* is used to refer to emails and other types of electronic messages sent via the Email System.
- *Users* are University staff, students and all other authorised users (such as consultants, guest lecturers, etc.) who are provided with a University email address including, but not limited to, an '@uclan.ac.uk' or '@lancashire.ac.uk' domain email address, and/or provided with access to the Email System.

B Scope of the policy

The policy applies to all Users of the Email System. It covers the use of the University Email System, including sending, receiving, storing and otherwise processing electronic messages and associated attachments. It may be referred to in the event of staff or student disciplinary action arising from, or involving use of, the Email System. Breaches of the policy will be treated seriously by the University and will be subject to sanctions under the University's Rules for the Use of IT Facilities.

C Responsibilities

All Users of the Email System must act responsibly and in line with this policy, any related policies (see section K for a non-exhaustive list) and any guidance which the University may produce from time to time regarding the acceptable use of electronic messages, Emails and the Email System.

The Information Governance Manager & Data Protection Officer, with support from LIS, is responsible for maintaining and updating this policy.

D Unacceptable use

Email and related services are provided by the University to support its primary purposes of education and research and their associated functions. Use of the Email System is granted to support these primary purposes and must be appropriate at all times. The University considers unacceptable use of the Email System to include (but is not limited to) Email and other electronic messages or attachments created or transmitted (including forwarding) which:

- bring the University into disrepute;
- infringe the copyright of another person or body, including intellectual property rights;
- contain any offensive, obscene or indecent images, data or other material;

- consist of unsolicited commercial or advertising material, chain letters or other junk-mail of any kind;
- are for the purposes of commercial activity or the carrying on of a business which is not related to the University's or the University's subsidiary companies' business purposes;
- inappropriately or unreasonably waste staff time or networked resources or which serve to deny service to other users;
- are intended to cause annoyance, inconvenience or needless anxiety;
- include material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;
- contain defamatory material;
- contain material which includes claims of a deceptive nature;
- by intent or otherwise, harass the recipient;
- violate the privacy of others or unfairly criticise or misrepresent others;
- are anonymous messages or deliberately forged messages or that have deceptive email header information (i.e. without clear identification of the sender);
- in the case of University staff or other workers paid by the University or its subsidiary companies, demonstrate excessive personal use of the system outside of the individual's own time.

E Research purposes

It is recognised that in the course of their work or research, Users may have a legitimate need to transmit or receive material which would normally constitute unacceptable use of the Email System. For the purpose of properly supervised and lawful research, it is acceptable to use the Email System in this way if approved in advance by relevant parties e.g. line managers and/or research supervisors and where appropriate ethical approval has been obtained.

F Personal use of the Email System

The University allows the reasonable use of Email and other electronic messaging for personal use, provided that the level of personal use is not detrimental to the main purposes for which the system is provided. Personal use means use for matters not related to University business. Users will adhere to the following guidelines when using the University's Email System for personal use:

- All personal emails must be clearly marked as such in the subject line, to distinguish between personal and business/study emails;
- Personal use of the Email System must not interfere with the work the University is paying you to undertake or the wider work of the University;
- Users must not use their University email address to create personal user accounts with third parties e.g. online shops, etc. The exception is where the account is required for activities related to University business or is required to confirm your student status e.g. to obtain discounts via a recognised provider of student benefits.
- Users **must not** use their University network password for accounts that are not provided by the University;
- Priority must be given to use of resources for the main purposes for which they are provided;
- Personal Email must not be for commercial or profit-making purposes or for any other form of personal financial gain;

- Personal Email must not be of a nature that competes with the University in business;
- Personal Email must not be connected with any use or application which conflicts with a User's obligations to the University as his or her employer;
- Personal Email must not contravene any of the University's rules, regulations, policies and procedures;
- Users must not forward chain letters, junk mail, jokes and executables;
- Users must not send mass mailings;
- Users must consider the size of attachments and keep them as small as possible;
- Users must remember that all messages distributed via the University's Email System - even personal Emails – are stored within the University Email System. Privacy of Emails and Email content (including attachments) cannot be guaranteed and should not be assumed; Emails may be accessed or monitored by LIS or other staff in cases where there is a legitimate business, employment or other need, as outlined in section G of this policy.

G Obtaining access to another User's Emails or Email account

Users will clearly mark personal (rather than business) Emails as such in the subject line of the emails to distinguish them from each other. Article 8 of the Human Rights Act 1998 (HRA) gives all individuals a right to privacy which extends to the workplace; as such, the content of personal Emails sent and received on the University Email System will not be accessed unless there is a legitimate need to do so. This right to privacy is not an absolute right; where the University can show that there is a legitimate need to access the content of a communication marked as, or likely to be, 'personal' in our Email System and can demonstrate that the resultant invasion of privacy is necessary and proportionate under the circumstances, it can be carried out lawfully in compliance with the HRA.

Email accounts, records and content of Emails sent and received by Users may be accessed (but not necessarily *intercepted* – see below) by LIS (including third-party service providers engaged by LIS), the People team, managers and other employees (such as colleagues in Legal and Governance, or colleagues investigating complaints) in cases where it is necessary for legitimate business, compliance or regulatory purposes, for the investigation of allegations of improper use or behaviour or to investigate alleged contraventions of any of the University's rules, regulations, policies and procedures, where it can be shown to be necessary and proportionate. They may also be accessed for the purposes of crime prevention and detection, the apprehension or prosecution of offenders or for actual or prospective legal proceedings or for the purposes of exercising, establishing or defending legal rights.

In some cases, it may be necessary for the University to *intercept* electronic communications such as Emails. Interception occurs when, in the course of its transmission, the contents of a communication are made available to someone other than the sender or intended recipient. It does **not** include access to stored Emails which have already been opened/read by the intended recipient. Where interception of communications is deemed necessary and appropriate, the University complies with the Investigatory Powers Act 2016 and the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (the Regulations). Under these pieces of legislation, it is lawful to intercept communications if:

- the interception takes place by, or with the express consent of, the University, as the system controller; and
- it is carried out for one or more of the purposes listed in the Regulations, which include:

- establishing the existence of facts e.g. to provide evidence that a specific piece of advice has been given;
- checking that the University is complying with regulatory or self-regulatory procedures that apply to University activities;
- checking that employees are working to acceptable standards while using the Email System;
- determining whether or not an Email is a business communication e.g. checking a person's Emails if they are on sick leave or absent for more than a few days to see if any relate to University business and need addressing;
- to prevent or detect crime;
- to ensure the security of the Email System and its effective operation;
- to investigate or detect unauthorised use of the Email System e.g. to monitor or investigate compliance with this policy.

Access to Emails and Email accounts (including where interception is necessary) may be granted in the form of direct access to a User's Email account or by specifying search parameters to LIS which result in the provision of individual Emails or other information. In the first instance, requests for any type of access will be made to LIS including the required justification, with guidance from the People team and Legal team, as required, to ensure such access is necessary and proportionate and has a lawful basis from data protection legislation. LIS will record information about the request and the reasons behind it, the extent and duration of any direct access to a User's account and who has been given access. Where appropriate, the User of the Email account will be advised of what has happened. Users granted access to another User's Email account under these circumstances will be made aware that Emails which are marked as, or appear to be, private or personal must not be accessed unless such access is necessary and proportionate under the specific circumstances of the case and must be treated confidentially.

If employees have shared team responsibilities and regularly need access to information sent to colleagues, they should consider whether or not a group mailbox may be appropriate instead of using individual Email accounts, as this may eliminate the need to request access to a User's Email account in the event of unexpected absences. Further information can be found in Appendix D.

H Security, data protection and confidential information

Emails are not a secure method of communication. They can go astray, be intercepted, be incorrectly addressed or be forwarded on to a number of people who are not entitled to see them within minutes. If the email is not protected, the information in it or attached to it will be disclosed to people who are not entitled to see it. When sending information by email, users of the Email System will take appropriate care to maintain the security and confidentiality of the University's information.

Users of the Email System – particularly employees – are likely to need to send confidential business information or personal data by email on a regular basis. *Personal data* is any information which relates to and identifies a living individual. It does not have to include their name. Data protection legislation requires the University to ensure that personal information remains secure and is not disclosed to people who are not entitled to see it. *Confidential or sensitive business information* is any information which relates to University business and has restricted access or is not suitable to be in the public domain.

To maintain security of personal data or confidential business information, it must be sent securely. Special category personal data; other personal data which could cause an individual damage or distress if it was inappropriately disclosed; or confidential or sensitive business information must be contained in an encrypted document or folder, which will then be attached to an email and sent to the recipient. Passwords must not be included in the same email as the encrypted attachment and Users must ensure that the recipient email address is correct. Users of the Email System with access to the staff intranet can find the guidance 'Sending personal information by email' on the Information Governance intranet pages, which should also be used as a guide for sending confidential or sensitive business information.

Using non-University email accounts

With the exception of Users sending their own personal data to their own email accounts, Users must not email any personal data, confidential or sensitive business information to their own Gmail, Hotmail or other non-University email account that they use, such as an email account provided by another organisation that employs the User at the same time as the University Personal or other non-University email accounts must not be used for University business and business data must not be sent or copied to personal or other non-University email accounts.

Using unapproved messaging tools

The University provides Users with the Email System to use for University business. This includes email accounts within Outlook and other messaging facilities approved for use by the University. Users must not use unapproved messaging tools to send Email for the purposes of University business. Examples of unapproved messaging tools include, but are not limited to, personal WhatsApp accounts, personal email accounts, SMS on personal mobile phones, and third party messaging platforms that have not been vetted and approved as a supplier under contract to the University.

Automatic forwarding rules

Users must not set up automatic forwarding rules on their University email accounts. If staff are out of the office, they should set up an 'out of office' auto reply using the template wording the University provides for corporate use. If staff regularly need to make their emails available to other members of their team, they should consider using a group mailbox for the team rather than granting access to their email account or setting up automatic forwarding rules (see Appendix D).

Malicious emails

The University uses tools and techniques, including phishing simulations, to protect against malicious emails such as phishing emails or those with attachments containing viruses and other malware. These tools are very effective but cannot stop all malicious or unwanted emails from being delivered to Users. Users will be directed to follow internal published guidance relating to identifying and handling malicious and unwanted emails, and will be encouraged to use reporting tools where available and to remain alert to the risks associated with malicious emails.

I Deletion and retention of Emails

The Email System is not a long-term storage facility. Users will be directed to actively manage Emails and delete messages as soon as they are no longer required for a specific activity or purpose, in line with the Information Management Policy. If information contained in an Email needs to be retained as a record of actions, decisions, discussions or information exchanged, it will be saved by the User to an appropriate University-managed location e.g. a structured repository on the University network, or a University-managed cloud storage location e.g. SharePoint, and then deleted from the Email System The University's Retention Schedule (available to Users with access to the staff intranet) provides direction about how long records relating to specific activities should be retained.

Users will be reminded to:

- Set their Outlook inbox preferences to empty deleted items when closing Outlook, which will permanently delete these items when Outlook is closed.
- Regularly review emails in the 'sent items' folder of Outlook, and any other folders within Outlook, to save any with ongoing value as a record, as outlined above, and delete those that are no longer needed for business purposes.

When a User leaves the organisation, any Emails which need to be retained for business purposes must be moved to an appropriate network or University-managed cloud storage location by that User or a nominated representative such as their PA. Further guidance on the maintenance and final disposal of email is available in Appendix B.

Information about the email storage space allocated to each user can be found in Appendix C. Storing information contained in Emails in an appropriate network or University-managed cloud storage location makes it easier to locate and retrieve the information when it is required again in the future and when it is due for destruction. Users will be made aware that any information they keep (whether or not it is required by the University) can be requested under data protection legislation or the Freedom of Information Act 2000 and may have to be disclosed to the person the information is about (if it is personal data) or into the public domain. This includes information and discussions contained in or attached to Emails.

J The Freedom of Information Act 2000

The University is a public authority and as such, is subject to the Freedom of Information Act 2000 (FOIA). The FOIA enables anyone, anywhere in the world, to request any information the University holds. Where there is a legitimate reason to withhold information which has been requested, an exemption may apply which means that the information may not have to be disclosed. Any information disclosed in response to a request under the FOIA is disclosed to the public as a whole rather than to an individual requester. Users of the Email System will be made aware that any information they send or receive by Email could be subject to a request under the FOIA (or the Environmental Information Regulations 2004, if it concerns environmental information), whether sending or receiving Email from internal or external sources. Information in Emails will not be retained if it is not required for business or legal purposes. Any information which does need to be retained will be stored appropriately on a network drive or University-managed cloud storage location such as SharePoint so that it can be located and retrieved easily in the event of an FOI request. Users will be made aware that once a request for information has been received by the

University, it is a criminal offence to intentionally delete information or documents to prevent their disclosure.

K Relationship with existing policies

This policy must be read in conjunction with the following policies, which are all available on the University intranet and/or external website:

- Data Protection Policy (and associated guidance)
- IT Security Policy (and associated guidance)
- Freedom of Information Policy
- Staff Handbook
- Regulations for the Conduct of Students
- Rules for the use of the University's IT facilities
- Social Media Policy
- Information Management Policy

Appendix A: Guidance on appropriate and effective use of emails

Email is an important business tool which is widely used across the University. It is important that users understand how to use email appropriately and effectively, to gain the most benefit from the system, protect the University from the various risks associated with it and enable staff and students to make the most effective use of their time. Following the guidance below will help ensure this happens.

Writing and sending emails

- Consider whether or not an email is necessary. Another method of communication may be more appropriate in some circumstances e.g. phone call.
- Remember that emails are the same as any other form of official communication. They can be taken to represent the views of the University when sent from a University email account and should be written with this in mind.
- Ensure you use the subject line in every email. Subjects should be brief and meaningful to enable recipients to determine the content of the email and decide if it is something which needs prioritising without necessarily having to read it.
- Create and use an email signature. Members of staff should use signatures which include their name, job title, phone number and 'University of Lancashire'. Any other relevant contact details can also be added. Outlook has the facility to create numerous signatures which can then be used at different times e.g. in cases where staff hold multiple roles.
- Write well-structured emails, keeping them brief, where possible.
- Use the spelling and grammar-checking tool before sending, with the language set to 'English (UK)'.
- Do not use smileys/emojis in business emails.
- Remember that your emails could be made public as a result of a Freedom of Information request or provided to an individual if the content is about that person. They could also be used

in legal proceedings. When writing emails, users should bear these in mind and only write emails which they would be prepared for individuals other than their intended recipient to see.
- Do not send unnecessary attachments. Compress large attachments (e.g. using 7Zip) before sending to reduce their size and their impact upon the system.
- Only mark emails as 'high priority', 'urgent' or 'important' if they genuinely are; the impact of using these markings will be reduced if they are used too often and inappropriately.
- When sending emails to a group of recipients, consider whether the 'Bcc' facility is more appropriate than the 'To' or 'Cc' facility. This could be the case where you are emailing a group who do not know each other and you need to ensure they can't see each other's email addresses or where it is not appropriate for each recipient to know who else has received the email.

Forwarding and replying to emails

- When forwarding emails, only copy in recipients who actually need to see the information and ensure you clearly state the action you require each of them to take.
- Consider whether or not it is appropriate to forward an email. Would the original sender expect this? Is the content private and/or confidential? Is it commercially sensitive and so restricted? Does it contain personal data which should not be further distributed? Ensure you only forward emails when there is a legitimate reason for another person to see the information.
- Reply promptly, even if it is just to explain that you are unable to respond in full at this point but will do so as soon as you are able.
- Consider whether or not it is appropriate to use the 'reply all' function. Do all the people who have been copied in to the email you have received need to see your reply? Only reply to those who actually need to see the information in your email.
- Ensure you don't use 'reply all' when you only intended to reply to the sender, particularly for sensitive or confidential emails. Particular care should be taken when replying from mobile devices where buttons are more difficult to select.

Checking email accounts

- Staff should check their email at least once each working day. If this is not possible, an appropriate 'out of office' reply should be turned on, stating when the account will be checked and who can be contacted in the meantime if the email needs urgent attention.
- Students should check their University email accounts frequently.

Email etiquette

- Be aware of how your email may be interpreted by the recipient. Ensure the tone and wording is appropriate and conveys your intended meaning and impression correctly. Email messages can easily be misinterpreted when there is no vocal intonation or facial expression to support your words.
- Do not use email to say something which you would not say to the recipient in person.
- Be aware that once you have sent your email, you have little or no control over who else may see it. It can be forwarded on to any number of recipients in a very short space of time. Ensure you only write things which you would be prepared for others to see.
- Do not use email to 'get something off your chest' to a large group of people all at once.

- Do not copy in members of staff e.g. managers simply to demonstrate that you have done something or asked for a piece of information from someone else, unless they have asked you to. Copying emails to numerous people unnecessarily increases the volume of emails within the system and means recipients who may not need to see an email must spend time reading them, potentially for no reason.

Appendix B: Maintenance and final disposal of email

Staff:	The email account will be locked once the end date specified in iTrent has been reached; the end date is determined and set by the People team. The account will be deleted 90 days after being locked. Following deletion, no mail will be retained. Schools and Services must retrieve any important documentation prior to staff leaving to ensure critical business information is retained and accessible.
Students:	Student accounts will be locked when a student is no longer entitled to a University email account based on the rules within Banner. The account will be deleted 60 days after being locked. No information will be saved or migrated from the email system.
Associate staff:	Account expiry dates are manually controlled in User Reg by LIS Customer Services. The account will be locked after its expiry date and deleted 90 days after being locked. Following deletion, no mail will be retained. Schools and Services must retrieve any important documentation prior to staff leaving to ensure critical business information is retained and accessible.
Contractors:	The email account will be locked once the end date has been reached in the User Reg system; account expiry dates are manually controlled in User Reg by LIS Customer Services. The account will be deleted 90 days after being locked. Following deletion, no mail will be retained. Schools and Services must retrieve any important documentation prior to contractors leaving to ensure critical business information is retained and accessible.

Appendix C: Quotas and limits

All users have access to the centrally-managed email system and all accounts have quota limits placed on them. No archiving will be in place and users are responsible for the housekeeping of their mailbox. The quota provided for each user is 50 GB.

Users receive an email notification when approaching their quota limit and are encouraged to follow guidance in the email to manage their account. Email that is received which takes an individual over their limit will always be delivered; however once over quota, no further email can be sent from an individual's inbox until they have reduced the storage below their limit.

There are limits on the size of an email that can be received and transmitted. These are set by Microsoft and may change over time.

Appendix D: Group Mailboxes

Specific group mailboxes can be requested for shared use if there is legitimate requirement. Requests for group mailboxes must be made to LIS Customer Services. The email address for the group mailbox must be meaningful to all staff and students at the University to avoid ambiguity. Access to the group mailbox must be strictly controlled, only providing access where there is specific business need for a user. Control of the mailbox is given to a specific nominated person when the mailbox is created; delegation of control is the responsibility of the user.