University of Central Lancashire
UCLan

Email use policy

Effective September 2020 - Present

Student Regulations and Policies

uclan.ac.uk/studentcontract

DOCUMENT CONTROL INFORMATION

CLASSIFICATION	DOCUMENT DESCRIPTION
Classification	Internal and external
Responsibility for drafting	Information Governance Manager & Data Protection Officer
Consulted with	Information Security and Data Quality Group
Approved by	Pro Vice Chancellor - Corporate Development
Effective from	April 2018
Next review date	As required following legislative or procedural changes
Enquiries to	Information Governance Manager & Data Protection Officer

This document is issued by Legal and Governance. Any copied or printed versions will be an uncontrolled copy. The definitive version is available from the Information Governance Manager & Data Protection Officer: DPFOIA@uclan.ac.uk

Contents

A Introduction and definitions

Email and other forms of electronic messaging are important and much-used services within UCLan. 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 staff about the management of the Email System, the expectations of privacy users of the 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.

In this policy, *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 Skype or Teams) and other similar communications including those sent via social media. *Email* is used to refer to emails and other types of electronic messages.

B Scope of the policy

The policy applies to all University staff, students and other authorised users who are provided with an '@uclan.ac.uk' domain email address or provided with access to other electronic messaging facilities provided by UCLan. It covers the use of the UCLan 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 UCLan 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 L 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. UCLan 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 UCLan's or UCLan'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);
- demonstrate excessive personal use of the system outside of the employee's own time.

E Research purposes

It is recognised that in the course of their work or research, individuals at the University may have a legitimate need to transmit or receive material which would normally be defined as offensive, obscene, indecent or similar. For the purpose of properly supervised and lawful research, it is acceptable to do so 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 by staff

UCLan 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. Users will adhere to the following guidelines when using UCLan's Email System for personal use:

- All personal (non-work) emails must be clearly marked as such in the subject line, to distinguish between personal and business emails;
- Personal use of email must not interfere with your work or the work of 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 an employee'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 UCLan's email system - even personal emails – are stored within the UCLan 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 Monitoring of the email system

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 UCLan 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 '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 employees may be accessed (but not necessarily *intercepted* – see below) by LIS, HR and managers in cases where it is necessary for legitimate business 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 by the intended recipient. Where interception of communications is deemed necessary and appropriate, the University complies with the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (LBPR). Under these pieces of legislation, it is lawful to intercept communications if:

- the interception takes place with consent of the sender and recipient; or
- it is carried out for one or more of the purposes listed in the LBPR, which include:

    - establishing the existence of facts e.g. to provide evidence that a customer has been given a specific piece of advice;
    - checking that the University is complying with regulatory or self-regulatory procedures;
    - checking that employees are working to acceptable standards;
    - 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 system and its effective operation;
    - to investigate or detect unauthorised use of the system e.g. to monitor or investigate compliance with this policy (NB: interception which is targeted at personal communications which are clearly not related to UCLan business purposes is not included and is not made lawful by the LBPR).

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 UCLan'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 UCLan 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 UCLan 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 will be contained in an encrypted document or folder, which will then be attached to an email and sent to the recipient. Passwords will not be included in the same email as the encrypted attachment and users will ensure that the recipient email address is correct. Users of the email system will comply with the guidance 'Sending personal information by email' (available to staff on the Information Governance intranet pages), when emailing personal data, which will also be used as a guide for sending confidential or sensitive business information. With the exception of students sending their own personal data to their own email accounts, users will not email any personal data, confidential or sensitive business information to their own Gmail, Hotmail or other personal (non-UCLan) email account. Personal, non-UCLan email accounts will not be used for UCLan business and business data will not be sent or copied to personal email accounts.

I Deletion and retention of emails

The email system is not a storage facility. Its primary purpose is for sending and receiving email messages and attachments. If any information contained in an email or attachment needs to be retained as a record of actions, decisions, discussions or information exchanged, it will be moved by the user to an appropriate network location e.g. a shared network drive such as the S drive or SharePoint then deleted from the inbox. UCLan's Retention Schedule (available to staff on the intranet) provides direction about how long certain classes of information should be retained. Users will set their inbox preferences to empty deleted items when closing Outlook, which will permanently delete these items when Outlook is closed. Folders will be cleared out regularly by users and information needed as a record saved, as outlined above. Any information which is not required will be deleted by users. Sent items will also regularly be deleted by users, once any emails required as a record have been saved. When a user leaves the organisation, any emails which need to be retained for business purposes will be moved to an appropriate network 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.

Deleting emails and the information they contain once they are no longer required saves storage space and reduces costs. 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 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 applicant. 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 mail 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 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 UCLan, it is a criminal offence to intentionally delete information or documents to prevent their disclosure.

K Third party access to email

Where a member of staff is away from the office for an unexpected or prolonged period of absence which could adversely affect the running of the University, LIS may provide access to an employee's email account for business purposes. In the first instance, requests for this type of access will be made by the employee's line manager and approved by the Head of Service or equivalent. LIS will record information about the request and the reasons behind it, the extent and duration of access and who has been given access. As soon as it is practicable and appropriate, the user of the email account will be advised of what has happened. Users granted access to another's inbox under these circumstances will be made aware that emails which are marked as, or appear to be, private or personal must not be opened or forwarded and must be treated confidentially.

If employees have shared team responsibilities and regularly need access to information sent to colleagues, they will consider whether or not a group mailbox may be appropriate instead of using individual email accounts. Further information can be found in Appendix D.

L Relationship with existing policies

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

- Data Protection Policy (and associated guidance)
- IT Security Policy (and associated guidance)
- UCLan's Acceptable Use Policy
- JANET's Acceptable Use Policy
- Freedom of Information Policy
- Staff Handbook

- Regulations for the Conduct of Students
- Rules for the use of the University's IT facilities
- Social Media Guidance
- 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 UCLan 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 Central 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 UCLan 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 HR. The account will be deleted where the expiry date was over 90 days ago and the last login was over 90 days ago. 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 where the expiry date was over 90 days ago. No information will be saved or migrated from the email system.
Alumni:	Alumni may request an alumni account from LIS CST (a charge may be applied for this). CST will manually set the expiry date in the User Reg system. The account will be locked after its expiry date and deleted where the expiry date was over 90 days ago and the last login was over 90 days ago. No information will be saved or migrated from UCLan's email system.
Associate staff:	Account expiry dates are manually controlled in User Reg by LIS Customer Support. The account will be locked after its expiry date and deleted where the expiry date was over 90 days ago and the last login was over 90 days ago. 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; the end date is determined and set by the account creator. The account will be deleted where the expiry date was over 90 days ago and the last login was over 90 days ago. 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.

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 Support. 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.