UCA Email Usage Policy

Version 1.2

Approved by: Director of IT Services
Date approved: 26/08/2020
Review period: Annual
Date reviewed: 26/08/2020
Owner: ITS Head of Networks, Security and Compliance

Table of Contents

1.0 Document Change Control

Version	Status / purpose of change	Author	Date
Draft		Janine Travers / Marion Wilks	25/08/2020
1.2	Update and reformat from previous policy	Janine Travers	26/08/2020

2.0 Overview

This policy and associated guidelines are intended to establish the necessary regulation for using email communications within the University and provide supporting information to ensure email is used in a compliant and responsible manner.

Compliance with this policy is necessary to ensure the protection of the University's reputation and success within academic, administrative and information sharing activities and to ensure business continuity, and minimise business damage by preventing and minimising the impact of security incidents.

This policy will be made available to all staff and student and anyone working for or on behalf of the UCA and made available on the UCA website.

3.0 Objectives

The objective of this Email Usage policy is to ensure that all email systems upon which the University depends are adequately protected to an appropriate level; ensure responsible usage and minimise damage by preventing and minimising the impact of security events and incidents.

Ensure compliance with all current and relevant UK and EU legislation, and ensure users are aware of the expectation and responsibilities in relation to these legislations and the associated University policies and procedures.

Review and enforce this policy and associated documentation

Ensure that this policy protects the University from liability or damage through the misuse of its email systems.

4.0 Scope

This policy applies to:

All members of the University (staff, students, external members of statutory committees); visitors to the University; partners with and sub-contractors to the University; and any other authorised users of the University's information.

The UCA and Ucreative domains that will be used for formal email communications; the University does not allow the use of alternative email addresses for the purpose of official business, this includes the forwarding of business emails to personal or non UCA accounts.

5.0 Roles and Responsibilities

Email Account Holder

Email accounts will be issued to a named individual on the authority of HR, a UCA representative or IT Services.

Any individual assigned a UCA email address is responsible for ensuring that the account is secured from theft or compromise of credentials or misuse and report any problems immediately to IT Services.

Shared Email Accounts / Mailboxes

Where an individual is granted access to a shared UCA email address or mailbox they have a responsibility for ensuring that their actions when accessing this mailbox are secured from theft or compromise of credentials or misuse, the mailbox is only used for its intended purpose and report any problems immediately to IT Services.

IT Services

IT Services are responsible for providing devices in good working order and will continue to monitor the status of the device to ensure that it meets the University's operating standards

All third party suppliers and contractors to the UCA who are granted UCA email accounts are to conform to this policy.

By using the University's e-mail facilities, all e-mail account holders accept the University regulations and policies pertaining to their use. The University has a legal responsibility to ensure that individuals with access to UCA e-mail act within the law by enforcing these regulations. Breach of the regulations constitutes a serious disciplinary offence.

6.0 Acceptable use and management of e-mail

a. Electronic mail (e-mail) is an integral part of the University's internal and external communication strategy and all staff have a responsibility to conform to its acceptable use. Staff also have a responsibility to be aware of the requirements of the Data Protection Act (DPA) and the Freedom of Information Act (FoIA) in relation to the use of e-mail; guidance is also available in the University's Information Security Policy and Information Handling Policy. Adherence to these policies and guidelines will ensure both effective communication and legal compliance.

b. All staff are expected to manage electronic messages effectively to expedite business communications, reduce paperwork and automate routine office tasks. It is the responsibility of staff to manage the creation, retention, and disposition of sent and received e-mails properly, including:
    i. Passing on messages for action and information to other staff as appropriate
    ii. Acting on e-mail as appropriate
    iii. Deleting e-mail and attachments as soon as they are no longer needed for reference in the e-mail system

c. The e-mail system must not be used for record keeping. All extant e-mails are discoverable under FoI and DPA. For long term accessibility, e-mails and their attachments should be stored on an appropriate network drive or UCA provisioned cloud storage. UCA will impose an automated deletion of email after a seven year period.

d. Sensitive personal data must not be communicated by e-mail unless express permission of the subject has been obtained or adequate encryption facilities are employed. The inclusion of personal data (including name and contact details) in an e-mail is deemed to be “processing personal data” within the terms of the DPA and the provisions of the Act apply. It is the responsibility of staff to ensure that they are familiar with the University's Data Protection Policy.

e. PCs and other devices must not be left in an insecure or unattended state that would allow another party to inspect e-mail or data and gain access to personal information.

f. UCA E-mail users are permitted to access e-mail on non UCA devices or connections (eg WiFi), however the user must ensure that the device or connection being used is sufficiently protected. If the device is a public device all credentials and history must be cleared and no attachments may be downloaded.

g. All staff are expected to set an “Out of Office message” for internal distribution that provides alternative contact arrangements . Be aware that the Out of Office message activated for external senders could pose a threat to individual security by communicating when individuals are on leave, use this feature with caution.

- When sending to multiple recipients users should build their own distribution lists or use the BCC field, ensuring that only recipients who should receive the email are on the list. Do not use the mass distribution groups such as “all staff” without prior approval from your Head of Department or School.

h. Personal comments about identifiable people should not be made in e-mails. The laws applying to defamation apply to e-mails, which are considered a form of publication. It is the effect of the communication rather than the intention of the sender that applies in cases of harassment.

i. The University e-mail system must not be used to create or distribute unsolicited, offensive or unwanted e-mails, including disseminating chain letters. If users receive jokes, chain emails, or other circulars by e-mail, these should be deleted and must not be forwarded either internally or externally.

j. E-mail messages that reflect badly on the University or could expose it to legal liability must not be sent. E-mails sent by a member of staff are equivalent to sending a letter on University headed notepaper and an equivalent level of care should be exercised.

k. Extreme care should be taken when downloading material from the internet, accessing URLs within e-mails, opening or responding to external e-mails if there is any suspicion that it might include a virus or malicious content. If there is any doubt, the IT Helpdesk should be contacted immediately.

l. All e-mails from external sources will be identifiable in the e-email content with the statement *'Warning: The sender of this email is external to UCA. Do not follow any links or open any attachments unless you are sure that the content can be trusted.'*

m. Use of the UCA e-mail system for personal communication must be kept to a minimum and not stored in the e-mail folders. The University computers must not be used for storing large personal media files. It is recommended that the UCA email address is not used for personal online accounts for example shopping sites.

7.0 Monitoring of E-mail

a. Neither the IT Services' staff and systems administrators nor any other members of the University will inspect individual UCA e-mail accounts unless there is a legal obligation which must be met or the University has approved a formal investigation.

b. Regular monitoring of the e-mail infrastructure is essential to ensure that the University IT Resources function effectively and are compliant.

c. In some circumstances it may be necessary to intercept e-mail traffic in order to specifically identify the cause of performance issues or system compromise. In such circumstances all reasonable steps will be taken to ensure the privacy of users.

d. Staff engaged in system support activities are bound by confidentiality clauses not to disclose any private information that they become privy to during the course of such activities.

8.0 Legislation and Standards

The list below contains some of the legislative and regulatory requirements UCA must comply with:

Data Protection Act 2018
The General Data Protection Regulation
Freedom of Information Act 2000
Human Rights Act 1998
Computer Misuse Act 1990

Companies Act 2006
Health & Safety at Work Act
Employment Legislation
Bribery Act 2010
Fraud Act 2006
Regulation of Investigatory Powers Act 2000
The Payment Card Industry Data Security Standard

9.0 Compliance

All members of the University have a responsibility to ensure that they are aware of and comply with this policy and all supporting University policies, procedures and guidelines. Each individual is responsible for protecting the University's information assets, systems and infrastructure.

Failure to comply with this standard could result in potential disciplinary action.

10.0 Related Policies, Standards and Procedures

- IT Use Policy
- Data Protection Policy
- Information Security Policy