Email Policy

Document Control

Responsibility for Policy:	Chief Information Officer
Approved by and date:	UEB 5th March 2024
Frequency of Review:	Annual
Next Review date:	February 2025
Related Policies:	None
Minor Revisions:	Clarification of policy particularly in relation to management of accounts upon leaving

1. Overview

Email services are provided by the University to support its primary role of learning & teaching, research and associated functions supporting these roles.

The University’s Email domain, @hope.ac.uk, is provided via G Suite for Education. This service is operated by Google.

Every member of staff is provided with an account when they commence employment. All students are also provided with an account when they register for a course. This account is the official means of communication between the University and the student.

2. Purpose

The purpose of this policy is to set out the acceptable use of the University's email and related services, systems and facilities. This will include responsibilities when using the University email service.

3. Legislation

All eligible users must comply with all applicable laws and regulations relating to the use of Email. This includes, but is not restricted to:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Copyright Designs & Patents Act 1988
- Malicious Communication Act 1998
- Criminal Justice & Public Order Act 1994
- Counter-Terrorism and Security Act 2015

4. Eligible Users

Staff

- All current staff
- Former members of staff where continued access approval has been granted by the relevant SMT member
- Designated other groups including, for example, council members and emeritus staff

Students

- Registered or pending
- Former students that have completed an Undergraduate or Postgraduate provision

5. Use of Email

- The University Email account should be used for University business only.
- Password Management

  Staff and student passwords for email should be unique and must not be the same as the one used to access their University network account or any other service (either University provided or private) utilised by the individual
- Users are responsible for reading and responding to their email in a timely manner.
- When using email, staff should try, wherever possible, to adhere to the guidelines set out in the email protocol.
- A very common method of distributing malware (Computer viruses, trojan horses and worms) is via email. Users must review the details of the sender of an Email to confirm that it is from a source known to the individual. Additionally, Email attachments should not be opened unless the user is confident that it is legitimate. In the event of doubt, the user should contact IT Services for guidance.
- Staff are responsible for setting up an automatic out of office reply through GMail when they are away from the University. This should include alternative contact details for urgent enquiries.

6. Unacceptable Use

Users of the Email service may not:-

- utilise the account for non-University business. In particular, it should not be used as the Email username or contact for private, non University account credentials
- create or transmit material which brings the University into disrepute
- create or transmit inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist or defamatory language or materials
- create or transmit material that encourages or endorses terrorist acts including those carried out in the past
- create or transmit material that could lead people to be drawn into terrorism or the promotion of hate or violence in any form
- create or transmit material which is designed or likely to cause annoyance, inconvenience or anxiety

- create or transmit unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind
- without authorisation, transmit to a third-party confidential material concerning the activities of the University
- transmit material such that this infringes the copyright of another person, including intellectual property rights
- engage in activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users
- engage in activities that corrupt or destroy other users' data or disrupt the work of other users
- create or transmit defamatory material or material that includes claims of a deceptive nature
- engage in activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals
- create or transmit anonymous messages or deliberately forge messages or email header information

It is recognised that, in the course of their work or research, individuals of the University may have a requirement to transmit or receive material that would normally be defined as offensive, obscene, indecent or similar. In the case of properly supervised or lawful research purposes, it is acceptable to do so. If in doubt advice should be sought.

7. Security and Privacy

- Google makes every effort to secure its service but cannot guarantee the infallibility of these systems to unauthorized intrusion, nor the authenticity of the sender of an electronic communication. For this reason, confidential or sensitive information should be contained in a password protected attachment and not appear in the main text of an email.
- Staff and students are responsible for keeping their email passwords confidential, and should never share this information with others, including friends and family members.
- Without prior notice, the University reserves the right, but not the obligation, to monitor and inspect individual accounts, files, and communications.
- If an employee is absent, the University reserves the right to access accounts in order to access emails and files to ensure business continuity.

8. Management of Accounts

Staff

- If an account for a staff member who is still employed by the University has not been accessed for a 12 month period, it will be suspended. Reinstatement of the account will only take place if approval has been received from the relevant authorised SMT member.
- When a staff member ceases employment with the University, the account will be suspended immediately. The Google Drive element of the account will then be reviewed by the School / Department owner (or their designate) and a request will be made to IT Services for the removal of access to or a change of ownership of the files.
- The leaver can request an extension to access the account that:
  - will have to be approved by the relevant authorised SMT member
  - will only be actioned once the review of the Google Drive ownership has been completed.
- Once a suspended account has not been accessed for a 12 month period, the account may be deleted and all the data removed.

Students

- Individuals who complete their studies on an Undergraduate or Postgraduate provision will retain access to their account subject to the following:
  - If the student does not access the account for a 12 month period, it will be suspended
  - Reinstatement of the account will only take place on request from the student provided that the student is registered on a course at that time.
- For all other cases, including for example students who do not complete the course and those on short courses / non-degree programmes, the account will be suspended at the cessation of studies.
- When an account has not been accessed for 2 years, the account may be deleted and all the data removed.

9. Enforcement

Any user who is found to have breached this policy will be subject to the University’s disciplinary policies.

10. Policy Review

This policy will be reviewed on an annual basis to identify any required revisions.