

Digital Communications Standard

August 2024

- [1. Standard Summary](#)
- [2. Scope](#)
 - [2.1. What does this standard cover?](#)
- [3. General Principles](#)
- [4. Account provision](#)
- [5. Statement of Individual Responsibility](#)
 - [5.2. Security & Privacy](#)
 - [5.3. Awareness](#)
 - [5.4. Duty of care](#)
- [6. Acceptable Use of Email accounts](#)
- [7. Other Services](#)
- [8. Personal use of your Email](#)
- [10. Communications etiquette](#)
- [11. If you need support](#)
- [12. Changes since previous standard](#)
- [13. Standards superseded by this document](#)

1. Standard Summary

- 1.1. The Email and Communications Policy establishes the college's expectations from employees in regards to their use of digital tools for communications purposes. This Standard details the measures which must be followed in maintaining compliance with that policy.

2. Scope

2.1. What does this standard cover?

- 2.1.1. This standard applies to all employees of the college (inclusive of external contractors and other third parties), in addition to the systems it owns and/or uses.

3. General Principles

- 3.1. Data Protection and Privacy by Design
- 3.2. Confidentiality Integrity and Availability (CIA)
- 3.3. Safeguarding of employees and students

4. Account provision

- 4.1. The college provides all students and employees with the use of a College Domain email account, with which to communicate within and without the organisation.
- 4.2. Except in specific circumstances (e.g. the requesting of a password reset or students with an IT Exemption approved by the Learner Support team), only a college-issued Email account which ends with @oca.ac.uk may be used for college-related Email communications. This is to ensure a level of accountability over individuals, and to ensure complaints and disputes that relate to behaviours relating to the content and/or frequency of Emails to be investigated.

5. Statement of Individual Responsibility

- 5.1. Individuals are themselves responsible for how they use their college Email accounts, and for the way in which they conduct themselves using digital communications more generally.
- 5.2. **Security & Privacy**
 - 5.2.1. College stakeholders who are provided with a college Email account are solely responsible for the security and privacy of

that Email account. Furthermore, employees of the college are required to maintain elevated levels of security for their Email accounts through the mandatory use of Two Factor Authentication with their Email account.

- 5.2.2. In addition, users of college email must never send or forward unsolicited email, and individuals email addresses must not be publicly disseminated through the Email 'To' field. Emails being sent to multiple individuals who are mutually unaware of each other must be sent through use of the BCC field or a relevant Email group.

5.3. Awareness

- 5.3.1. Individuals who find themselves in receipt of spam, or spoof email, or email which might potentially contain viruses or other damaging content, are responsible for not proliferating such messages to the wider college community and are required to notify the college's IT Services Team (ithelpdesk@oca.ac.uk) as soon as possible.

5.4. Duty of care

- 5.4.1. Individuals in possession of an oca.ac.uk Email account have a duty of care over its use. Avoid subscribing to dubious services or mailing lists using the Email account, and apply caution to subscribing to overseas services or mailing lists that are not in compliance with UK Data Protection Act 2018 or EU General Data Protection Regulation 2016 (GDPR).

6. Acceptable Use of Email accounts

- 6.1. The College's main purpose in providing Email accounts is to support the teaching, learning, research and approved business activities of the College. Email accounts should not be abused. Abuse, for the purposes of this standard includes (but is not necessarily limited to):

- Creation or transmission of material which brings the College into disrepute.
- Creation or transmission of material that is illegal.
- The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind

- The unauthorised transmission to a third party of confidential material concerning the activities of the College.
- The transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users.
- Activities that corrupt or destroy other users' data or disrupt the work of other users.
- Unreasonable or excessive personal use.
- Creation or transmission of any offensive, obscene or indecent images, data or other material.
- Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or anxiety.
- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature.
- Activities that violate the privacy of others or unfairly criticise or misrepresent others.
- Creation or transmission of anonymous messages or deliberately forging messages or email header information, (ie without clear identification of the sender) or for 'flaming'.
- The unauthorised provision of access to College services and facilities by third parties via use of your Email.

7. Other Services

- 7.1. Your Email account provides you with Single Sign-On access to a range of services associated with the College.
- 7.2. These include but aren't limited to: learn.oca.ac.uk, discuss.oca.ac.uk, media.oca.ac.uk, oca.padlet.org, and other Google Workspace services (such as Google- Meet, Drive, Calendar, Chat and Sites).
- 7.3. These services and platforms are monitored by the college for activity and content which may be in breach of college policies or relevant laws relating to misuse of systems, e.g. [The Computer Misuse Act 1990](#)

8. Personal use of your Email

- 8.1. Within reason, you are permitted to use your OCA Email account and associated services for personal use. For example, for subscription to newsletters or services of appeal, which are not of an illegal or ethically questionable nature.
- 8.2. Your OCA Email account will provide you with highly discounted rates on various services unrelated to your degree, e.g. Amazon Prime, Spotify, Apple products and Adobe software; there are no restrictions on your use of the OCA Email account for obtaining such discounts.
- 8.3. Your Email account also provides you with benefits through the *Google Workspace for Education* range of services, including cloud storage through the Gdrive service.
- 8.4. You are not permitted to use college-provided storage for personal use or for storing and transferring copyrighted material, such as published music or video files, or copyrighted images for which you have no specific consent to possess. Furthermore, college-provided services must not be used for any form of illegal file sharing either within or without the organisation. Breach of this policy may result in disciplinary action being taken.

9. Account Quotas & Limits

- 9.1. Your Email account has an upper attachment limit of 25MB. However, attachments of up to 5TB can be uploaded through use of the Gdrive attachment option in the Gmail web interface. When using this method of attaching files please ensure that:
 - sharing permissions are correctly set (it will default to everyone at the Open College of the Arts with the link has

access, this can be changed to 'Only recipients of this email can View'),

- that the file or files contain no harmful code/viruses and,
- you have permission to share the files being uploaded.

10. Communications etiquette

10.1. When engaging in any form of digital communications with other individuals, the following guidelines should be adhered to:

- 10.1.1. In video calls, basic etiquette rules should be followed, including muting microphones when not speaking, using appropriate virtual backgrounds, using the 'raise hand' function rather than speaking over others, and wearing appropriate, inoffensive attire.
- 10.1.2. College staff hosting or participating in video calls should conduct themselves in a professional manner, in the same way that they would in an in-person office-based meeting.
- 10.1.3. Only arrange video calls where an email chain or chat would not suffice.
- 10.1.4. Be mindful of the data privacy rights of all video call participants (invited but not attending as well as present) when engaging in discussions; all participants may receive recordings or transcripts following the call, so Data Privacy should be considered at all times.
- 10.1.5. For simple ad-hoc questions or informal discussions, consider using Chat, rather than Email to avoid cluttering inboxes.
- 10.1.6. In text-based communications, avoid using: all caps (shouting); underlining; font colours denoting urgency; potentially offensive imagery.

11. If you need support

- 1.1. For support with interpretation or adherence to this Standard or associated Policies, please contact ithelpdesk@oca.ac.uk or raise a ticket at helpdesk.oca.ac.uk.

12. Changes since previous standard

- 12.1. This is the first version of the Digital Communications Standard. All Information Security Policies and Standards will be revised as part of an ongoing ISMS project.

13. Standards superseded by this document

- 13.1. This is the first version of the standard as a separate document. It supersedes any standards previously contained in V2 of the Information Security Policy set.