Imperial College
London

Imperial College

Code of Practice 2: Electronic Messaging

Doc. Ref.	: Code of Practice 2: Electronic Messaging
Version	: 4.1
Status	: In Review
Date	: 24 March 2022
Approved by	: The Information Governance Steering Group
Review by	: 31 March 2024

1. INTRODUCTION AND DEFINITIONS

1.1 Electronic communication applications, including e-mail and calendar are important means of communication for the College and they provide an efficient method of conducting much of the College's business. This document sets out the College's guidelines on the proper use of electronic communication applications for College purposes, including teaching, research and administration. It describes the practices, rules and regulations, specifically in reference to security and data protection.

1.2 Imperial College use Office 365 service from Microsoft to provide an electronic communications platform which includes use of “Office” software by its staff and students. This guideline is intended to provide information about the use of electronic communications systems, including, but not limited to Outlook, Skype for Business, Teams, and Yammer.

1.3 A “message”, as used in this document, is defined as any piece of written communication, attachment, recording, picture, or any other file sent, received or published using electronic communications software.

2. SECURITY

2.1 The contents of all email accounts may be accessed subject to approval through normal College process with reasonable cause as explained in Paragraph 11.9 of “Conditions of Use of IT Resources (Acceptable Use Policy)” in the College’s Information Security Policy.

2.2 Electronic mail and calendars are not secure services. For example, it is possible for unauthorised individuals to monitor the transmission of e-mails or calendar items, or to send counterfeit mail under a user's name. Therefore, users must not include any confidential or personal information in an electronic message unless the information is encrypted. Please see Be Secure (IT Security) on how to share confidential or personal information securely.

2.3 To enhance collaboration, calendar items including their subject lines may be available by default for other College staff to see. Therefore, staff and students must avoid putting any sensitive (including personal) information in the subject line of calendar items. The notes within a calendar item will not be visible to others by default including attachments. However, you should still avoid putting any sensitive or personal data in calendar items as per section 1. For a full list of sensitive data and protected personal characteristics see the College’s Information Security Policy and Data Protection Policy respectively. Also note that, other personal information could be deemed as sensitive depending on the circumstances, e.g. names of people attending interviews, leave types of staff (such as hospital appointments, domestic emergencies), etc. Subject lines of any private calendar entries could be made invisible to others by selecting the “padlock” icon to make them private.

2.4 College e-mail accounts are accessible everywhere with the use of the “Outlook Web App” on any web browser software. When “Outlook Web App” is used, the session will time out after 1 hour when not active to avoid someone else gaining access to the account. After this duration, the system will require re-authentication by entering the user name and password.

2.5 Please take care when addressing email communications, and consider

that the Autocomplete function may suggest a different email address to the one intended. If you send personal or sensitive personal data to an incorrect email address, please report this as a data breach using the reporting data breaches procedure.

2.6 If you are sending emails to multiple recipients with sensitive content where it may be a data breach for recipients to be identifiable by each other, please make sure that you use the "blind copy [BCC]" field, instead of "To" or "CC".

3. ARCHIVING, RETENTION AND DELETION

3.1 All messages older than 2 years will be automatically moved to archive folders for new users. To search/find emails older than 2 years, users have to go to the "online archive" section. One of the following options can be selected to change this setting using the "Assign Policy" option under the "Home" menu:

- Do not archive (All e-mail messages will be kept in the default folders in Outlook (e.g. Inbox and Sent Items) and will not be archived automatically.)
- Archive e-mails older than 2 years.

3.2 E-mail messages will normally never be deleted. The following options are available to College users to select from:

- Delete messages older than 5 years
- Delete messages older than 10 years
- Retain all messages indefinitely

3.3 If you select any of the "delete" options, your messages older than the specified number of years will be regularly purged without further notice.

3.4 When a staff member or student leaves the College, their account will be soft-deleted, that is, disabled on the date of their departure. The email account will no longer be accessible. Six months after the departure date, the accounts will be fully deleted, which will trigger the complete purge of the mailbox after another 30 days. Staff members may request to retain their College user name/email account for continuity of College business for up to six months. This must be authorised by their line manager and the Director of ICT.

3.5 There is a College policy and process that allows line managers to access staff members' emails and files for continuity of College business after they have left. Staff members are encouraged to delete all personal emails and files before they leave.

3.6 When a student (undergraduate or postgraduate or postgraduate researcher) leaves, ICT will offer them an Alumni email account on Google Mail on the "@alumni.imperial.ac.uk" domain. They will receive the information about the "Google email address for life" and they will be able to set this up if they prefer to do so.

4. USE OF NON-COLLEGE EMAIL AND EMAIL FORWARDING

4.1 College staff and students are provided with College email addresses for email communication to be carried out in a safe and reliable way, and give

a level of assurance that emails have been delivered. This assurance cannot be provided in the case of College staff and students using an external (non-College) email accounts to carry out College communications and auto-forwarding of emails to an external email account. Therefore, using an external email account to carry our College business and auto-forwarding to external (non-College) email accounts are not permitted.

4.2 If you believe you have a valid reason to redirect your College email to an external email account, please raise a ticket with the ICT Service Desk and this will be reviewed in line with the College's Information Security Policy. Staff with redirects or auto-forwards to "nhs.uk" accounts will be allowed to keep these if they declare they do not have access to their College email accounts from their usual work place.

4.3 Emails of staff who have privileged access to one or more College systems (e.g. System Administrators, DBAs) as well as staff with financial approval responsibilities must NOT be auto-forwarded under any circumstances.

4.4 For students, email auto-forwarding is only available after they have completed their studies and for the duration their College email account is kept active.

5. OTHER

5.1 The College provides access to e-mail systems for the conduct of the College's business. Incidental and occasional personal use of e-mail is permitted within the College so long as such use does not disrupt or distract you from conducting the College's business (i.e. due to volume or frequency) or prevent others from accessing the network for legitimate College business.

5.2 Trade Union representatives who are members of the College may use the e-mail system to transact union business with their members.

5.3 All staff and students are encouraged to upload a recent photo of themselves as an icon photo to allow people to identify them on Microsoft Office 365 environment. However, if you prefer not to share your picture publicly, you should not use a picture other than a true reflection of yourself and should leave the icon picture as default.

Version History

Version/Status	Release Date	Comments
1.0/Approved	January 2013	Approved
1.1/Revised – In Review	April 2016	Fully revised version following findings report by Information Governance Audit in 2015 and Implementation of Microsoft Office 365
1.2/In Review	July 2016	Reviewed by John Neilson, College Secretary and Mike Russell, CIO; section 2.3 added regarding personal information on calendar item subject lines
1.3/In Review	July 2016	Reviewed by IGSG.
2.0/Approved	November 2016	Approved by the Provost Board
2.1/In Review	April 2018	Reviewed by Okan Kibaroglu, Tim Rodgers and Matthew Williams. 2.5 reference to information security incident changed to data breach Section 3.4 updated and new 3.5 added in line with the new Leavers form Section 4 updated to reflect new policy and regulations regarding auto-forwarding of emails
3.0/Approved	May 2018	Published
3.1/In Review	March 2019	Reviewed by ICT Governance and Security. Paragraph 2.6 added to use BCC when sending sensitive emails to multiple recipients.
4.0/Approved	January 2021	Published linked to InfoSec policy v6.0
4.1 In review	March 2022	Amendments to URLs