# Email Acceptable Use Policy

## 2023/24

BLOOMSBURY
INSTITUTE
LONDON

# Index

# Document Version Control

| Document Version | Committee | Committee Action | Date |
|---|---|---|---|
| V6.0 | SMLT | Approved | 6 July 2022 |
| | | **Date in force** | **25 July 2022** |
| V7.0 | SMT | Approved | 5 July 2023 |
| | | Date in force | **1 September 2023** |

The Email Acceptable Use Policy will be reviewed annually by our Senior Management Team (SMT). Any amendments will be subject to approval by the Senior Management Team.

# 1. Introduction

Email is the key mechanism for communication of official institutional information to students. In many cases it is becoming the default means of communication reducing the cost and environmental impact of paper-based communications.

This Email Acceptable Use Policy applies to all staff (including temporary staff), Student Guild, visitors, contractors, consultants and students using our IT facilities and resources. Those using the IT facilities and resources provided by Birkbeck College under the terms of our arrangement with Birkbeck College are expected to abide by the latter's IT policies whilst on their premises as well as abiding by our own.

This policy should be read in conjunction with our other policies (including our Internet Acceptable Use Policy)[1] and UK and international law. See Appendix A for details of the UK legislative framework within which we operate. Please note that the contents of this policy are not intended to contradict or contravene UK or international law.

The purpose of this policy is to set out acceptable use of email by students, staff, the Student Guild, visitors, contractors and consultants using our IT facilities and resources. It is intended to:

- ensure that the content of any email communication does not constitute a breach of any institutional policies or the legislative framework within which we operate.
- ensure that any message has a high chance of delivery, thereby improving the chances of it being read, while reducing the inconvenience to users.
- reduce the likelihood of outgoing email being regarded as Spam by recipient systems.
- eliminate problems or complaints regarding the service.

# 2. Principles

The following principles draw upon research into best practice in the area and the guidelines offered by the large providers, including Google, Hotmail, Yahoo and AOL. These principles should be followed in order to ensure compliance with our policies and the legislative framework within which we operate including compliance with the Prevent duty. They should also be read in conjunction with our Communication Principles which can be located in the Communications library on SharePoint or by emailing our Deputy Head of Marketing, Communications and UK Student Recruitment (Communications Lead) for a copy.

# 3. Information for staff

Use of email by staff is permitted and encouraged where such use is suitable for business purposes and supports our goals and objectives. Email is to be used in a manner that is consistent with our standards of business conduct and as part of the normal execution of an employee's role within the Institute.

Bloomsbury Institute email accounts are to be used for our business and email messages are treated as potential corporate messages. Bloomsbury Institute may directly access staff email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation. Limited personal use is considered acceptable.

The introduction of the Student Self-service Portal (SSP) allows students to maintain their own contact details. It is important that all staff use this student contact email information for all email correspondence with the students.

[1] www.bil.ac.uk/qem/policies

Bloomsbury Institute reserve the right to redirect the email of staff that have left or who are on long term leave for legitimate business purposes. Only members of SMT / SLT will authorise email redirect requests. Use of email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.

Staff should be conscious that anything they write in an email may be subject to disclosure under the Freedom of Information Act 2000 or Data Protection Act 2018.

Staff must set up an out of office reply if they are going to be away from work for whatever reason, for half a day or longer. The out of office reply should state when staff will return to the office and, where possible, who to contact in their absence.

Staff should only contact enrolled students via their Bloomsbury Institute @bil email account. The only exception to this is if they are responding to a communication submitted via the Student Self-service Portal (SSP).

# 4. Information for students

New students will be automatically allocated Bloomsbury Institute email addresses, and their personal contact email address will be collected during the admissions process. Students are informed of the purposes for which their email address will be used, and informed of the "no publicity" flag, which will be used to reduce offence caused by Unsolicited Bulk Email (Spam).

Students are responsible for maintaining their contact email address via the Student Self-service Portal (SSP). This needs to be communicated to all students. All students will, in any case, be asked to confirm/update their contact email address as part of the annual on-line re-enrolment process.

No messages should be sent from anonymous email addresses or invite a response to an unmonitored mailbox.

Use of multiple addresses for the same student is not permitted.

# 5. Email lists

Email lists based upon set criteria can be created within our student management system and shared among the relevant staff. Sending to the distribution list can be restricted if needed. This facility is ideal for large recipient groups, and where periodic messages are being sent to the same groups of recipients. Additional distribution lists may be requested from IT Services (ITS).

Staff distribution lists are available through the email system and the Divisional and Departmental Heads are responsible for updating these distribution groups regularly. This facility is suitable for messages sent to recipients numbering up to a few hundred, but limitations in the email client may restrict larger recipient lists, and a distribution list should be used.

Students' contact information (first name, last name, Bloomsbury Institute email address) is held within the VLE. Staff and students using the VLE may send to selected students or groups. Mass communications or notifications shall come within the scope of Tier 2 Communications and shall be subject to our Information Control Procedures[2].

# 6. Specific guidelines for use

## 6.1 General

- Staff and students are expected to check their Bloomsbury Institute email accounts on a regular basis.

[2] www.bil.ac.uk/qem/policies

- The email etiquette is that employees do not send emails outside of 8 am to 8 pm Monday to Thursdays and 8 am to 6 pm on Fridays. They should also refrain, wherever possible, from emailing at weekends.

- Staff responses to staff emails should be within 1 working day [the response can be just a 'holding reply']. Staff should respond within 5 working days following any holding reply.

- Staff responses to student emails should be within 2 working days [the response can be just a 'holding reply']. Staff should respond within 5 working days following any holding reply.

- Users should not open any attachments received from unsolicited sources in order to prevent the transmission of viruses.

- Users should ensure that the device is locked or logged out when left unattended to prevent unauthorised access and use.

- An email will only be deemed confidential if it is labelled as such, however it will still be subject to any Freedom of Information Request received.

- Never reply to spam.

- Do not send any scripts and avoid HTML emails if possible. System generated emails containing HTML, supporting business processes, are acceptable.

- Do not use an old email to initiate a new email exchange because the subject in the title box will be misleading later.

- Be careful when replying to emails previously sent to a group. With such emails, refrain from using "Reply All" unless your reply is relevant to every individual within the group.

- Archive effectively - use folders and delete any messages no longer needed.

- Do not overuse the "URGENT" flag as it will lose its value.

- Avoid using email for sensitive messages or messages that may prompt an emotional response.

- All inbound mail to your Bloomsbury Institute account first passes through a mail filtering system

- The Institute recognises that spam and phishing emails are a significant problem and have taken various precautions to minimise the impact of these messages by applying filters to reduce the incidents of unwanted mail. In addition, all incoming messages are checked for spam and viruses by an external message filtering service (Barracuda Essentials). Messages identified as spam or suspicious are quarantined. Users are provided with the option of reviewing these messages to ensure that they have been correctly identified and to release any of the messages for forwarding to their email accounts.

## 6.2 Content of the message

- Take care in drafting emails, considering any form of discrimination or harassment, Institutional representation, data protection issues and the legislative framework within which we operate.

- Draft emails with the same care as letters, as staff emails are a form of corporate communication.

- Re-read messages before sending to check for clarity and to make sure that they contain nothing which will embarrass the organisation or make it liable.

- The email must be relevant to the recipients.

- Where appropriate, emails from staff to students should be personalised if possible.

- Chain messages should never be forwarded.

- Subject lines must accurately describe content.

- Those sending emails should never ask for personal information or passwords in emails.

- Avoid the use of 'PS' or the inclusion of additional information after the end of the main body of the email. Such text can often be overlooked by the reader, especially if the reader has any form of visual impairment.

- Great care should be used when linking to HTTP URLs, which should not link to IP addresses or non-standard ports.

- Messages should include an email "signature" with sender and institutional contact details. The signature must follow institutional guidelines which staff can obtain from the Head of Communications. Staff should sign their emails with their name and not just the email signature.

- Messages should also open with a greeting or salutation.

- Academic staff should include their office hours in their email signature.

- Avoid images in email where possible – include ALT tags on all images that are sent.

- Send email in plain text format where possible.

- Use file compression techniques for large documents or send them using an alternative method.

## 6.3 Email addresses and addressees

- The email addresses of other recipients should never be revealed.

- Use only Bloomsbury Institute addresses in the "From:" and "Reply-to:" header addresses. They must be valid addresses capable of receiving email.

- Use shared mailboxes if appropriate, rather than individuals' addresses for sending email.

- When using the shared mailboxes, the sender must include their name in the signature on behalf of the Department/Division.

- Understand how to use CC and BCC: only CC in people that really need to receive the email.

- When permission from all within the group has not been received for their email addresses to be viewed by other members within the group, use BCC.

## 6.4 Bulk emails or mass emails

- Use distribution email lists where possible.

- Avoid 'Mail Storms' - long discussions sent to a distribution list - consider verbal communication or use a bulletin board.

- In case of sending bulk email or mass email, keep all the recipients' email addresses in BCC.

- Bulk email or mass email should be tailored and targeted to smaller groups of recipients where possible.

- Bulk email or Mass email communications must follow our Information Control Procedures[3]. These emails require prior approval before they are sent out.

## 6.5 Unacceptable use or behaviour

It is unacceptable to:

- Solicit emails that are unrelated to business activities or are for personal gain.

- Send or receive any material that is obscene or defamatory, or which is intended to annoy, harass or intimidate another person. See our Dignity and Respect Policy and Harassment and Sexual Misconduct Policy[4] for further information.

- Send or receive any material that is linked to a proscribed terrorist organisation or information that generally promotes or incites acts of violence or terrorism. See our Prevent Policy[5][6] for further information.

- Represent personal opinions as those of the Institute.

- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the Institute, or the Institute itself.

- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, databases and the information contained therein, computer network access codes, student information and business relationships.

# 7. Dealing with complaints

- Complaints relating to non-delivery of messages will be investigated by the ITS team but are limited to establishing whether the recipient mail servers accepted the message.

- The relevant member of staff should respond by email to any student complaints or requests raised through the Student Self-service Portal (SSP).

- Messages which generate an NDR (Non-Delivery Report or bounced message) must be acted upon.

- "Permanent" error messages must be acted upon immediately.

[3] www.bil.ac.uk/qem/policies

[4] www.bil.ac.uk/qem/policies

[5] www.bil.ac.uk/qem/policies

- Individuals may request that they that they stop receiving emails, however where this email is for the proper performance of the work of the Institute or the management of staff then we may not accept this request.

## 8. Monitoring and sanctions

We accept that the use of email is an extremely valuable business, research and learning tool. However, misuse of such a facility can have a detrimental effect on other users and potentially our public profile. The distribution of any information through our network is therefore subject to scrutiny. We reserve the right to determine the suitability of email content and any illegal use of the email service will be dealt with appropriately.

Accordingly:

- We maintain the right to access user email accounts in the pursuit of an appropriately authorised investigation.
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
- We are obliged to monitor to fulfil our responsibilities with regard to UK law. Referrals will be made to the Head of IT Services and, where relevant, the Prevent Lead as appropriate.
- Action (including disciplinary action) may be instigated, as deemed appropriate, by the Head of IT Services and the Deputy Chief Operating Officer.

## 9. Related policies and procedures

- Dignity and Respect Policy
- Information Control Procedures
- Internet Acceptable Use Policy
- Information Security and Management Policy
- Prevent Policy
- Staff Departures: IT Procedures
- Staff Disciplinary Procedures

## 10. Review

The Email Acceptable Use Policy will be reviewed annually by our Senior Management Team (SMT). Any amendments will be subject to approval by the Senior Management Team.

# Appendix A: Legislative framework for our Email Acceptable Use Policy

The following list is not exhaustive:

- Communications Act 2003
- Computer Misuse Act (1990)
- Counter-Terrorism and Security Act 2015
- Criminal Justice and Immigration Act 2008
- Criminal Justice and Public Order Act 1994
- Data Protection Act (2018)
- Equality Act 2010
- Freedom of Information Act (2000)
- UK General Data Protection Regulation 2021 (UK-GDPR)
- Human Rights Act (1998)
- Malicious Communications Act 1988
- Obscene Publications Act 1959
- Prevent Duty Guidance (2015)
- Regulation of Investigatory Powers Act (2000)