

# Email Use Policy Introduction

This email use policy describes the rules governing email use at the College. It also sets out how staff

members are expected to behave when using email. And to ensure that employees:

* comply with current legislation
* use email in an acceptable way
* do not create unnecessary risk to the College by their misuse of the internet

This policy should be read alongside other key policies, in particular users should also read the College Data Protection and Social Media policies.

# Scope

All employees of Homerton College when using their College/University CRSID email account.

It applies to the use of email accounts tied to the College/University on any device, whether or not it is owned by the College or the employee.

It applies no matter where the email use takes place; on College premises; while travelling for business or while working from home.

# Business email use

The College recognises that email is a key communication tool. It encourages its employees to use email whenever appropriate e.g., communicating and/or distributing information to students, College and University staff, customers or suppliers.

All College business performed via email should be conducted through Microsoft Outlook and using College/University CRSIDs. All Homerton employees and workers who are expected to use email as part of their day to day work will be provided with an Outlook account and a CRSID.

Employees should only use email accounts provided for them by the College or University when conducting College business. Employees should not use personal email accounts when conducting College business.

# Personal use of email

The College also recognises that email is an important tool in many people’s daily lives. As such it allows employees to use their College CRSID email account for personal reasons, with the following stipulations:

* Personal email use should be kept to a reasonable level, sent and restricted to non-work times, such as breaks and during lunch
* All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate whether or not it is be being sent or received for business or personal use.
* Personal email use must not affect the email service available to other users. For instance, sending exceptionally large files by email could slow access for other employees.
* Personal emails should be transmitted with a personal signature not representing the College.

# General administration of emails

## Email branding and disclaimer

All emails should follow the College branding as outlined on the Y drive.

## Out of office message

Employees should always action an out of office message on their email account if they are expected to be absent from work during normal working hours for more than 24 hours, preferably with an alternative contact email or telephone number.

An out of hours message would normally apply during periods of holiday absence but, if possible and when appropriate, a message should also be actioned during periods of sickness absence.

## Tenure of emails

Employees using email should ensure that they regularly review, archive and delete their emails that they receive and send. Employees are encouraged to use the Outlook ‘Mailbox clean up’ function located in the Account Information page of the ‘File’ tab on a regular basis to facilitate this.

Emails should be stored and retained only as long as the data held within it is of value to the College and/or in line with statutory or College retention periods for the same or similar data which is held within databases and manual filing systems. See retention schedule for further information.

Email is a transitory medium used to facilitate the communication of information. If the value is expected to be more long term, the information should not be stored in email. An alternative secure medium should be identified and used in line with statutory and College retention periods.

## Retention schedule

Email and connection log data will be retained for 6 months, after which it will be destroyed.

# Email Security

Used inappropriately, email can be a source of security problems or breaches for the College. Employees must always consider the security of the College’s systems and data when using email.

Users should note that email is not inherently secure. Most emails transmitted over the internet are sent plain text. This means they are vulnerable to interception. Although such interceptions are rare, it is sensible to regard email as an open communication system not suitable for confidential messages and information.

Users of the College email system are advised **not to**:

* Automatically reply to a long thread of emails without reviewing the content of all previous messages and whether it is appropriate for the existing recipient list. Wherever possible avoid ‘replying to all’, ‘blind copying’ (bcc) and remove any previous messages if in any doubt.
* Change the subject of an email when replying to a message. Always start a new email where there are new recipients.
* Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.
* Disable security or email scanning software. These tools are essential to protect the College from security breaches.
* Send confidential College data via email. If this is the only suitable means available, documents should always be password protected and the password sent under separate email or by a different form of communication e.g., telephone.
* Access another user’s College email account. If an employee requires access to a specific message (for instance if an employee is off sick or has left the College) the employee should approach their line manager or the IT Department.

If required, help and guidance on email security is available from the College IT Department and Data Protection Officer.

# Inappropriate email content and use

The following behaviour by an employee is considered unacceptable:

* Using College communications systems for setting up personal businesses or sending chain letters.
* Forwarding of College confidential messages to external locations.
* Creating or distributing any inappropriate content1 or material via email.
* Accessing copyrighted information in a way that violates the copyright.
* Breaking into the College's or another organisation’s system or unauthorised use of a password/mailbox.
* Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.
* Transmitting unsolicited commercial or advertising material.
* Introducing any form of computer virus or malware into the corporate network.
* Use of College communication systems for any illegal or criminal activity.
* Distributing messages or material that could damage Homerton College’s image or reputation.

Any user who receives an email that they consider to be inappropriate should report this to their line manager.

# Monitoring

The College’s email resources are provided for legitimate business purposes. Therefore, the College maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the College also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed by the IT Committee.

# Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the College's disciplinary procedure. If the employee is found to have breached the policy, they may be given a

1 *Inappropriate content includes: pornography, racial or religious slurs, gender specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.*

*This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religion or political beliefs, national origin, disability, sexual orientation or any other characteristics protected by law.*

disciplinary warning up to and including termination of employment as outlined in the College’s disciplinary policy. The level of warning applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

**AMENDMENT CONTROL SHEET – Email Policy**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section/Page** | **Rev. No.** | **Date** | **Description** | **By** | **Approved** |
|  |  |  |  |  |  |