Email Policy

Purpose and Scope

ICON College provides all students with an email account for academic purpose and also to ensure one dedicated channel of communication with them.

The purpose of this Email Policy is to set out the conditions under which the College's email system should be used.

The policy applies to all current students, ex-students, employees and third parties using ICON College email address.

Responsibilities for Email Accounts

- All users of the College's email system are responsible for the security of their mailboxes and must not share the access to the mailboxes. Students are responsible for all activities that occur within their accounts.
- If a user becomes aware that any unauthorised access has taken place, he/she should notify the college immediately emailing on support@iconcollege.ac.uk.
- Any emails sent by the College to the students will be delivered to their College email addresses (name.lastname@iconcollege.ac.uk) and students must ensure that they check their accounts regularly.
- Any member of staff, if is a current student of the college must not use their student email account for administrative activities purpose, instead staff email account should be used
- Students should be aware that every email address and associated account – whether used by a current or former student – is the property of the College. Students and alumni must remove all their personal emails and any items of a personal nature that they wish to retain from their email account in advance of it being closed. The College email account will be closed within 6-9 months of the course completion date.
- All email account holders should comply with the email policy, and staff with responsibilities for students should be aware of its requirements.

Legislation

The users of the College email system are obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to all the users of the College email system users, who may be held personally accountable for any breaches.

The users for the College email system shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Regulations
- Privacy and Electronic Communication Regulations
- The Computer Misuse Act (1990)
- The Copyright, Designs and Patents Act (1988)
- Equality Act 2010
- Protection of Children Act 1978
- Obscene Publications Act 1959
- Malicious Communications Act 1998
- Investigatory Powers Act 2016

Data Protection

The College is the domain administrator for College email system (@iconcollege.ac.uk) and administers all email accounts in accordance with its Data Protection regulation. For details refer to College's data protection policy.

Acceptable Use

The College's email account provided to all students for academic purposes and for the duration of their studies. They are also permitted to continue to use the account for up to 9 months after they have left the College. After this time the email address will be retired from use.

The College permits the personal use of college email for a reasonable level of personal use. Authorised users of the College's email system must use its email account responsibly, complying with all relevant policies and laws.

Prohibited Use

The College's email system must not be used for (this is not an exhaustive list):

- the creation, transmission or storage of text, images and other material that is offensive, obscene, indecent, discriminatory, harassing or libellous;
- the transmission of material that infringes the intellectual property rights of another person, including copyright;
- use the email system for any unlawful, invasive, infringing or fraudulent purpose;
- the creation or transmission of material that brings the College into disrepute;
- the incitement of violence;
- activities that corrupt or destroy other users' data or disrupt the work of others;
- activities that violate the privacy of others or unfairly criticise or misrepresent others;
- unauthorised personal financial gain or a commercial or profit-making nature;
- generate or facilitate unsolicited bulk commercial email;
- intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;

Monitoring

This policy and its implementation will be subject to internal monitoring and auditing, and the outcomes from these processes will inform and improve practices as a part of a commitment to continual improvement.

- The College will carry out monitoring of email systems for regulatory compliance and to protect against cyber-attacks.
- Account activity logs (e.g. logins, usage, storage etc) are monitored and all messages are routinely scanned (for viruses, spam and other security threats) to assist with the effective operation of the email system.
- The routine monitoring may be carried out by the College, or by an authorised third party on behalf of the College. In the event of an identified cyber-attack, human intervention and access to emails may be required.
- The College, as the domain owner and administrator ties, may use analytical tools to monitor the email server and have access to information held in an email account. The College reserves the right to access this information in the following circumstances:
- to investigate a complaint, where relevant;
    - to investigate a reasonable suspicion of abuse of computer facilities;
    - to cooperate in the investigation of a crime;
    - in an emergency situation, including as a response to a potential cyber security incident.

  Otherwise, the College will respect the privacy of all email account holders.

An audit trail of system access and data use by email administrators and students are maintained and reviewed on a regular basis.

Security

The emails like all other methods of communication, cannot be assumed to be secure. Therefore, the College undertakes following measures, to minimise the risk of interception or breaches of confidentiality.

- Students are responsible for the security of their individual mailboxes and must not disclose their passwords to others.
- Although emails are routinely scanned for virus content and spam, students should take reasonable measures to prevent the introduction and transmission of computer viruses, including:
    - not opening attachments received from unsolicited or untrusted sources;
    - not transmitting attachments known to be infected with a virus;
    - ensuring that antivirus/anti-spyware software is installed and updated regularly on any computer used to gain access to the IT systems in the College.
- The unauthorised interception of, or access to, the messages of others is illegal.
- The IT Support (support@iconcollege.ac.uk) should be informed immediately if a suspected virus is received or a student becomes aware that someone has gained unauthorised access to his/her account.

Managing email accounts

- Each student will be provided with an email account.
- The address for the account will be based on the individual~~’s~~ student name and surname (e.g. Firstname.surname @iconcollege.ac.uk).
- Any technical queries related to the email should be directed to support@iconcollege.ac.uk
- All emails sent by the College to the students will be delivered to their college email addresses, and it is important that the accounts are checked regularly.

Non-Compliance

Compliance with this policy is the responsibility of all members of staff and students.

Any breach of the policy may result in disciplinary action or access to the College’s facilities being withdrawn.