CHURCHILL COLLEGE
CAMBRIDGE CB3 0DS

IT Facilities, the Internet and Electronic Mail Policy

Policy Name	IT Facilities, the Internet and Electronic Mail Policy
Purpose	This policy sets out appropriate use of IT systems within the College, the use of internet access provided by the College and the use of electronic mail provided by the College.
Owner	Head of IT
Contact	Head of IT (David Spaxman)
Approved By	College Council
Approval Date	8 October 2024
Next Review Due	MT2027
Version and Recent Changes	V1 as an independent policy MT24. Previously part of the Staff Handbook.

IT Facilities, the Internet and Electronic Mail Policy

1. Introduction

1.1. This policy has been created to lay out an acceptable agreement on the appropriate use of IT systems within the College, the use of internet access provided by the College and the use of electronic mail.

2. Scope

2.1. This policy applies to all users of College IT Systems, even if they have not been specifically given their own personal account to use.

3. Use of IT Facilities

3.1. IT facilities are provided for a variety of uses including academic use (Fellows and students), administrative use (employees) and for some limited Conference uses.

3.2. The use of IT facilities is governed by separate sets of rules issued by the party providing them: College IT systems are issued by the College, University systems by the University Information Services (UIS) and so forth. College IT facilities may also be further constrained by relevant rules issued by UIS, owing to the nature of the College IT system's reliance on some aspects of the University IT systems.

3.3. The administrative IT facilities are provided for College business only and are not for personal use. Personal use consists of the use/storage of personal files, photographs, videos, documents and any other types of files or actions that are not considered part of your job role within the College, or as part of College business.

3.4. All users of the administrative IT facilities must use these in accordance with the College's Data Protection Policy, Data Security Policy and related procedures. When using these facilities employees should follow the College's guidelines on data hygiene. Employees will also be required to set up Multi-Factor Authentication (MFA) or 2 Factor Authentication (2FA) methods as part of accessing administrative IT facilities for the first time, which provides additional protection for them.

3.5. The College retains the right to access any electronic files held on equipment owned by the College and provided for College purposes. This will usually be authorised by an employee's direct line manager, their seniors or members of the HR department.

3.6. It is also important that employees do not hold College data on their own personal devices, unless expressly given permission to do so by the College IT Department.

3.7. All users of the administrative IT facilities shall be expected to treat any information which may become available to them through the use of these facilities with appropriate confidentiality.

4. Use of The Internet

4.1. Use of the Internet for personal purposes is not permitted during working hours. However, reasonable use may be made of the College facilities outside working hours for personal purposes so long as there are legitimate reasons for doing so.

4.2. For security reasons, no user should visit a website if there is any reason for suspicion about its content. (For example, many virus-generated emails and "spam" emails encourage their

readers to visit specific websites either without reasonable justification or with misleading justification. Web sites advertised in this way must be avoided. If you have any concerns about an email or website, please seek advice from the College IT Department.)

4.3. The internet must not be used to access offensive or illegal material, such as pornographic material, or material that promotes racism or other forms of hatred, or terrorist, or extremist materials.

5. Electronic Mail (E-Mail)

5.1. Use of the College email facilities and accounts for personal purposes is not permitted. This includes named college mailboxes (e.g. Joe.Bloggs@chu.cam.ac.uk) as well as shared (e.g. Porters@chu.cam.ac.uk) and role (e.g. hr.manager@chu.cam.ac.uk) mailboxes.

5.2. Staff should not consider any College email accounts, whether named, shared or role, to be private. College e-mail addresses should not be set to auto-forward to a non-College email address. The College may, when necessary, access any account or auto-forward emails to an alternative account.

5.3. Employees must never use email to send or forward messages that are defamatory, obscene, abusive, or otherwise inappropriate. Any employee doing so could face disciplinary action and in serious cases this could be regarded as gross misconduct and result in summary dismissal.

5.4. When writing emails, employees should always think very carefully about what they write, about the tone of their email and should write them as if they will be read by others, not just the intended recipient. Employees should remember that if an individual makes a Data Subject Access request, anything an employee has written concerning an individual will have to be revealed. This applies equally to communications sent via messaging services, e.g. a text message sent from a work mobile phone.

5.5. Employees should ensure that appropriate official College information is given on any emails that they send – for example: job title, contact details, registered charity number etc.

5.6. Employees should exercise care not to copy emails automatically to all those copied in to the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person. Care should be taken when sending emails to ensure these are sent to the correct intended recipient. Sending personal data to an incorrect recipient may constitute a data breach. If employees believe this has occurred they should report this via the College's Data Breach reporting procedure.

6. Breach of Policy Monitoring and Results

6.1. Subject to the constraints laid down by the Regulation of Investigatory Powers Act, the College may monitor web pages accessed by an individual, email messages sent and received by an individual and any other activities of an individual on the network and/or using the College's IT facilities.

6.2. Monitoring of an employee's email and/or internet use will be conducted in accordance with a privacy impact assessment that the College has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the College's legitimate interests and is to ensure that this policy on email and internet use is being complied with.

6.3. If an employee is found to not comply with this policy disciplinary action may be taken, up to and including dismissal for gross misconduct and/or they may be liable to prosecution.

To minimise the risk to the College, use of College IT facilities, electronic mail and the internet, and compliance with this policy, is monitored.

7. Related Documents

i. Data Security Policy
ii. Data Protection Policy
iii. Bullying and Harassment Policy