Information Services

Birkbeck Information Security Policy

Supporting Policy 3: Birkbeck Staff Electronic Communications Policy

Approved by Strategic Planning Committee

20 September 2022

0. Context

This policy forms part of the Birkbeck IT Regulations. For more information, contact Birkbeck IT Services, a link to their contact details is available on the Birkbeck IT Regulations page.

1. Introduction

The Birkbeck Acceptable Use Policy sets out for all users the acceptable use of College IT facilities.

The purpose of this policy is to set out acceptable use of email, internet and telephone facilities by staff. Guidance is also provided regarding the circumstances under which interception and or retention of copies of communications or monitoring of an individual's use of these facilities may occur. The policy is intended to make staff aware of their obligation to use such IT services responsibly, professionally, ethically and lawfully and to make them aware of the rights and activities of the College with regard to the monitoring of such systems. The guidance provided should help to safeguard the interests of both members of staff and the College.

2. Scope

This policy applies to all staff of the College. It applies where staff are using email or the internet in connection with their work for the College, whether within or outside of normal working hours, and whether or not using College owned or supplied facilities or personal devices such as smartphones and tablets.

3. General Principles

The College encourages the use of electronic information systems such as the internet (including social media) and email systems. It is recognised that such forms of electronic communications are essential to the work of the College and provide a range of benefits, such as increased access to information resources, improved communications, increased flexibility for a better work/life balance, and improved information and knowledge sharing. However, staff should be aware that improper use of email and internet activities may have adverse consequences for themselves or the College, such as lost productivity, reputational damage to individuals or the College and potential breaches of the law. Examples of potential breaches of the policy are provided in the College Computing Regulations and could include posting of defamatory or libellous messages, divulging personal data, breaching copyright, and accessing illegal content.

The policy aims to protect both staff and the College from potential risks associated with the use of email, internet and social media. If a staff member is found to have acted in breach of this policy this may lead to disciplinary action being taken against them, up to and including dismissal.

The IT and telecommunication facilities are primarily provided for official College business. Such College systems are therefore not to be considered private by its users albeit that the College attempts wherever practicable and reasonable to safeguard the privacy of its employees and users. It is recognised that there are occasions when employees might legitimately make reasonable use of their telephone, email or Internet access for personal purposes. Such reasonable personal use is permitted as long as it does not interfere with the performance of the employee's duties, does not incur unreasonable cost to the College, nor cause damage or difficulty to the College's IT facilities, nor any difficulty or distress to others. Guidance on what constitutes 'reasonable' use is given in the sections below.

College staff should be aware that this policy forms part of the Birkbeck IT Regulations.

The College reserves the right to update this policy from time to time.

4. Email

Email is an important and efficient means of communication which is used to conduct much of the College's business. All College staff will be provided with a Birkbeck username and email address of the standard form: name@bbk.ac.uk. All email communications on College business must be sent and received using this account.

You should note that centrally maintained distribution lists (such as staff@bbk.ac.uk) operate on the standard address assigned to staff.

You must ensure that emails you send internally or externally comply with College policies. In particular:

- You must not send offensive email including any form of harassment, discrimination or bullying. Senders of such emails are subject to normal disciplinary rules. Note that unlike purely verbal communications, with email it is normally possible to supply evidence to support a complaint. If you receive an obscene, racist, sexist or defamatory email, whether unwittingly or otherwise and from whatever source, do not forward the email to any other address, except (upon request) to a member of the College IT Services staff.
- You must not knowingly make any inaccurate, defamatory or libellous statements in your emails. An email message is legally equivalent to a letter and can form contracts. For these reasons it is important to take the same care composing email messages as letters. Email messages, like other documents, may also be liable to be disclosed to the person they are about under the Data Protection Act 2018 or in the event of legal proceedings.
- You must not infringe a third party's intellectual property rights by sending protected material without the necessary rights to do so or without crediting the owner.
- You must not imply that your message contains the official policy view or intent of the College if it does not.
- You must not send messages purporting to come from someone other than the actual sender (spoofing) or an appropriate role account.
- You must not send out unsolicited bulk email messages (spam).
- You must not share personal information without taking adequate precautions in the content of the message or any attachments.
- You must not breach data protection when sending emails. Be careful not to disclose personal data (such as email addresses) in a bulk email. Use the bcc (blind carbon copy) functionality to protect the privacy of the recipient email addresses.
- You must check your email account regularly.

Where the College has reasonable grounds to suspect misuse of email in terms of either the scale of use, or the content or nature of messages, it reserves the right to intercept (if necessary) and to monitor the email including but not limited to the destination, source and content of email. The use of email (for either personal or business purposes) to send or forward messages or attachments which are in any way defamatory, obscene, or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure.

4.1 Personal Use

You are strongly advised to use personal email accounts for personal communication. However, you may make reasonable use of the College's facilities for personal emails, provided that this does not have more than a minimal impact on resources and does not adversely affect your work and the work of others.

4.2 Privacy

Emails sent through the College email system form part of the official records of the College; they are not private property and may be disclosed under the Freedom of Information Act 2000 and Data Protection Act 2018, as part of legal proceedings and as part of disciplinary proceedings. Members of staff are responsible for all actions relating to their email account and should therefore make every effort to ensure no other person has access to their account.

You should also note that all email is intrinsically insecure unless it is encrypted, therefore you should use discretion if information of a confidential or sensitive nature is being considered for transmission by email. You should also note that copies of email messages are left on computer systems at key stages in the delivery process.

Subject always to the College's rights and the statement about the qualified nature of the privacy afforded to employees and users of the College's electronic information systems, a user's email account and the data associated with it is principally private. You must not attempt to access or read another user's email unless specifically authorised by the owner of the account to do so. In the case of permission being given, for example to a personal secretary to access email for a member of staff, care must be taken to ensure that third party personal data is not comprised, whether by breach of confidentiality or otherwise.

4.3 Access to account in the absence of the account holder

Any access to the IT account in the absence of the account holder will be done according to the IT Account Monitoring and Access Policy. A link to the policy can be found on the Birkbeck IT Regulations page.

4.4 Accounts of Staff Leavers

Staff Leavers accounts will be dealt with according to the IT Account Monitoring and Access Policy. A link to the policy can be found on the Birkbeck IT Regulations page.

4.5 Storage and Backup

The storage and backup of emails is done according to the IT Backup and Logging Policy. A link to the policy can be found on the Birkbeck IT Regulations page.

4.6 Junk Mail (Spam) and Phishing Emails

Some of the incoming emails received by College users may be unsolicited, some may be unwanted and some may be dangerous in containing viruses, worms, etc. It is also increasingly common to receive phishing emails used by fraudsters to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity. The College recognises that spam and phishing emails are a significant problem and ITS have taken various precautions to minimise the impact of these messages by applying various filters and virus protection software at the mail hubs and central servers to reduce the incidents of unwanted mail. In addition, all incoming messages are checked for spam and viruses by an external message filtering service. Messages identified as spam 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 College email accounts.

The following should be observed by all users:

- Beware of all emails from unknown sources, especially those containing attachments. Delete such messages without opening them. Please also note that emails sent from known sources may have been sent by a virus infected computer, so please watch out for all suspicious email.
- Do not forward or reply to chain emails, offensive messages or those offering products or services. In some cases it is not advisable to respond to an offer to be removed from the distribution list of these messages as such action will identify to the sender that the email address is in active use by a real person and may lead to further junk email.
- If you are unsure whether a message is fraudulent, you should check with IT Services.

5. Internet and Social Media

The College is committed to allowing its staff the freedom to access the Internet and the Web for the easy retrieval of information in order to carry out their learning & teaching, research or administrative role within the College.

You may make reasonable use of the Internet and Social Media for other than strictly work purposes provided it does not adversely affect your work and the work of others and has a minimal effect on the College's resources. Limited, occasional or incidental use of the Internet for personal purposes is understandable and it is recognised that there can be times where it is sensible for the employee to make occasional use of the Internet for personal reasons such as a private transaction (e.g. carrying out a bank transaction or booking a holiday), rather than having to spend considerably more time out of the office. Such personal use should be confined to non-working hours and must not interfere, either

by its timing or extent, with the performance of your duties. Staff who abuse this privilege will be subject to disciplinary action.

For centrally provided systems, IT Services keep records of account logins and web activity logs.

You should be aware that the College reserves the right to monitor network traffic in order to ensure that its facilities are not being used for inappropriate purposes. In particular you **must not**:

- Deliberately access material, which is counter either to legislation, College policies or to commonly accepted standards, or is likely to be offensive to reasonable people. This includes, but is not restricted to, any sexually explicit or violent material or sites which promote racism or intolerance. It is possible that accidental access to such material or sites can take place. If you are concerned that such accidental access has taken place you may wish to report your concerns to your line manager.
- Attempt to gain unauthorised access to any computer or computer system, whether belonging to the College or any other organisation or person.
- Download executable files for non-work related purposes. These include programs, applications, utilities, screen savers, games, etc. Where files are required for work purposes, the appropriate care to guard against virus infection must be taken, and the software properly registered and paid for where appropriate. You should contact IT Services or your local IT support staff for any assistance.
- Download or use any data, programs or other software or system facilities in a manner that breaches the licence agreement between the College and the service provider. It is the responsibility of every user to be familiar with licence conditions, and if in any doubt to verify the position with IT Services or your local IT support staff.

The College recognises that the use of social media and online social networking is an increasingly useful communication tool that provides a positive way to exchange ideas on common interests, collaborate with other academics and professionals as well as keep in touch with friends and colleagues. The College increasingly uses multi-media approaches to attract, engage and communicate with current and prospective students, staff, partner organisations and other stakeholders and in order to promote Birkbeck's brand and reputation. Some staff members also contribute to the college's social media activities as part of their role, for example by writing blogs, managing a Facebook account or running an official twitter account.

Use of social networking sites not related to work purposes is allowable so long as it is reasonable, proportionate and does not interfere with work. Such access should be limited to breaks and outside of normal working hours.

Staff members should follow the College's 'Principles for the use of social media by Birkbeck staff and students', a link to which can be found on the Birkbeck IT Regulations page.

6. Telephone

The College telecommunication facilities are provided primarily for business use. The College does not record or monitor the content of telephone calls made using its equipment.

You should be aware that summary call usage information is routinely provided to designated telephone representatives in Schools and Administrative Departments for recharging purposes.

Staff are normally expected to use their personal mobiles to make personal calls during non-work hours. However, the College recognises the occasional need for staff to make or receive short personal calls on College telephones (both fixed line and mobiles), but this privilege must not be abused.

Staff with a College business requirement can request the supply of a College-supplied mobile phone. The issue of these devices is subject to the agreement of the budget holder responsible for the relevant School / Department cost-centre to which initial and recurrent charges will be recharged. Authorisation of the Executive Dean or Head of Professional Services Department is also required to confirm the business requirement. Online monthly statements from the network provider are provided for information and reimbursement of any personal charges (if relevant, e.g. international roaming charges).

Where the College has reasonable grounds to suspect possible misuse of its telecommunication facilities, it reserves the right to monitor the destination and length of outgoing calls and the source and length of incoming calls. This would not normally involve the surveillance of calls but in certain rare circumstances, where there are reasonable grounds to suspect serious misconduct, the College reserves the right to record calls.

7. Monitoring of Email, Internet and Telecommunications

The College monitors and records the use of its IT facilities according to the IT Account Monitoring and Access Policy, a link to which is available on the Birkbeck IT Regulations page.

8. Version Control

Version	Date	Author	Comments
1.0	June 2016	ITAG	Initial version
2.0	June 2017	ITAG	Amended
2.1	10 November 2020	Reviewed by Abu Hossain	Content rearranged. Minor edits. References to other policies updated.

2.2	2 March 2021	Reviewed by James Smith	Suggested updates regarding the monitoring section.
2.3	29 April 2021	Reviewed by Abu Hossain	Moved the monitoring sections from different policies including this policy and created a separate policy. Policy name changed according to the naming convention. Added the context section.
2.4	5 May 2021	Reviewed by Abu Hossain	Moved the storage and backup content from this policy and created a separate policy.
2.5	14 February	Marion Rosenberg	Minor edits for clarity and consistency. Renamed Staff Electronic Communications Policy
2.6	September 2022	Marion Rosenberg	Minor edit to section 4 to ensure in line with earlier communications on email use.