**Birkbeck Policy on Staff Use of Email, Internet, and Telephone Facilities
(considered by ITAG June 2016 and amended June 2017)**

**1. Introduction**The College Computing Regulations (available at: <http://www.bbk.ac.uk/its/regulations/birkbeck-college-computing-regulations.pdf>) provide guidance to all users on the acceptable use of College computing facilities.

The purpose of this policy is to set out what is regarded as acceptable use by College staff of email, internet and telephone facilities. 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.

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 smart phones, tablets and iPads.

**2. 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.

The College's IT Services (ITS) routinely monitor the overall patterns of usage of the College's IT and telecommunication services. It does not, in the normal course of events, specifically identify the use made of facilities (with the exception of telephone usage for departmental recharging purposes) by any individual member of staff. However, all staff should be aware that the College keeps logs of email, internet and telephone usage. Where duly authorised in accordance with this policy, ITS will investigate potential misuse or abuse of these facilities. The circumstances under which such activities may be undertaken are outlined in Section 6. Cases of computing or telecommunication misuse by College staff will be referred to the College authorities to be dealt with according to the relevant staff disciplinary procedures.

College staff should be aware that this policy on the acceptable use of email, internet, and telephone facilities complements existing guidelines relating to the use of College IT facilities. Such guidelines include the College Computing Regulations and the College Network Security Policy. Both of these are available from the HR pages on the College Intranet at:
<http://www.bbk.ac.uk/hr/policies_services/policies_az/computing_regulations> and
<http://www.bbk.ac.uk/hr/policies_services/policies_az/networksecurity>

The College reserves the right to update this policy from time to time. Any amended policy will be made available on the HR policy pages of the College intranet.

**3. 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; or from an equivalent School account in the form: name@department.bbk.ac.uk.

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

You must ensure that emails that you are sending internally or externally comply with College policies.
In particular,

* You must not send offensive email encompassing all or 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 support 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 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).
* You must not send out unsolicited 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 (refer to Section 6). 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.

**Personal Use**You are advised to use personal email accounts for personal communication, but 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. Any member of staff found to be spending lengthy periods of their working day using the email system for non-work related purposes will be subject to disciplinary action.

**Privacy**Emails sent on 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 and Data Protection Acts, 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.

**Access to email in the absence of the account holder**The College reserves the right to access a staff member’s email account in the unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the staff member’s role.
Such access should, in normal circumstances, be carried out with the prior knowledge of the employee. However, where impracticable, inappropriate or if the employee is not readily contactable, then the College reserves the right to access the employee's email account for business related information.

Requests for access to a staff member’s account should be made to the ITS Service Desk its@bbk.ac.uk by the staff member’s line manager, stating the name of the absent member of staff, the length of time access is required and the reason for requesting access. This will be logged as a Service Desk call and passed for approval as appropriate (by the relevant Executive Dean, Head of School, Director of Professional Services Department, Director of IT Services or the HR Department).

Requests can also be sent to activate the “Out of Office Assistant” on the email account of the absent member of staff. Such requests should include the suggested text of the “Out of Office Assistant” message.

**Accounts of Staff Leavers**Staff leaving the College should ensure that any non-business-related messages have been removed from their College email accounts. Access to your Birkbeck computer and email accounts will end automatically following your last day of service. Should you require access beyond the end of your employment, please liaise with your line manager. The request must be made by your line manager (or appropriate College authority) and e-mailed to the IT Service Desk (its@bbk.ac.uk) who will provide an extension for a defined period. Retiring academics and researchers with a continuing association with the College can request an extension by contacting the ITS Service Desk (its@bbk.ac.uk) who will provide extended access for an agreed period.

**Storage and Backup**All email messages sent from or received by user accounts of the standard format; i.surname@bbk.ac.uk from external recipients; pass through central mail hubs. A log is kept of the transaction (sender, receiver, date/time, subject, etc.) but not the content. This data is kept for a minimum of 1 year. ITS, as part of its data storage policy, automatically backs up all user files on central systems on a daily basis and retains backed up data for business continuity purposes (with daily weekday backups being retained for a month, and monthly backups retained for one year).

All users should consider the need to retain emails relating to College business for an appropriate period of time, bearing in mind statutory retention periods for specific types of information. Staff should consult ITS or Faculty/School support staff with advice on the archiving of email communication if they wish to retain such data outside of their active email systems.

ITS will normally retain email accounts on the centrally managed Exchange system of staff leavers for a period of three years (under review). These may include personal email messages if these have not been deleted prior to the departure of the staff member. All retained emails are stored securely with access limited by the Head of School or Professional Services Department or his/her designate.
**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 for a period of 14 days. 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 guidelines 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 the ITS Service Desk.

**Best Practice Guidelines**College users should be aware of best practice guidelines for when sending emails. These are available on the ITS web http://www.bbk.ac.uk/its/services/email/staff/services/email/emailgoodsite at:

<http://www.bbk.ac.uk/its/services/email/staff/services/email/emailgood>

**4. 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 ITS keep records of account logins and web activity logs. ITS retain account login information on use of central systems for a period of 1 year.

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 your ITS or Faculty/School 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 ITS or Faculty/School 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 for 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’** which are available at:
<http://www.bbk.ac.uk/registry/policies/documents/social-media-principles.pdf>

**5. 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. Telephone call records are retained for a period of 1 year.

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 out-going 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 (refer to Section 6).

**6. Monitoring of Email, Internet and Telecommunications**As has been stated above, the College's email, internet and telecommunication systems are provided for business use, and as such the College reserves the right to monitor the use of these facilities. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (the “Regulations”) are ancillary to the Regulation of Investigatory Powers Act 2000 and allow organisations to intercept, monitor and or retain communications transmitted over their systems without consent, but having notified its users of the circumstances in which such action may take place, which the College is hereby doing, for the following purposes:

* Establishing the existence of facts
* Ascertaining compliance with regulatory practices or procedures
* Preventing or detecting a crime
* Investigating or detecting unauthorised use
* Ensuring the secure and effective operation of the system.

The College considers that from time to time each of the above circumstances are relevant to the College’s operation and the use of its electronic and other systems, and as such reserves its rights as afforded to it under the Regulations.

As stated in part 3 above under the section titled Junk Mail, the College routinely intercepts emails using automated systems and scans them for viruses and other malicious software or code, and to determine whether or not the same appears to be unsolicited mail. It should be noted however that the College does not routinely monitor the content of information stored or transmitted in electronic format. It will normally only undertake monitoring of an individual's email, internet or telephone usage (and content where appropriate) in order to investigate potential misuse or abuse of these facilities. The consent of the individual member of staff, whilst not required where the law and/or this policy specifically permit the College to monitor its email, internet and telecommunications systems, will normally be sought unless,
(a) urgent access is required for operational reasons; (b) there is evidence that a member of staff may be misusing facilities to a serious extent which, if corroborated, could result in disciplinary action; or, (c) there is a need to investigate and there is a serious possibility that evidence may be destroyed.

Save as set out in this or other relevant College policy requests for the monitoring of an individual's use of IT and telecommunication services or the content of such communications require the explicit authorisation by a member of the College's Senior Management Team (usually the College Secretary or designate). Following such approval, the monitoring will be undertaken by designated staff within ITS acting, for operational reasons, under the direction of the Director of ITS. These staff are required to observe the strictest confidentially when undertaking these activities and they will record or monitor only to the extent necessary to establish the facts of the case. These reports will be made to the College Secretary who in consultation with the HR Director will determine the actions that need to be taken in any particular case.

Information obtained through monitoring will only be used for the purpose for which the monitoring was carried out, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore. By way of example, breaches of health and safety rules that put other workers at risk.

The College does not carry out any covert monitoring of its staff. It would only undertake such covert monitoring of staff if, having taken advice, it considered that it was justified and had been specifically authorised by the College Secretary or designate. The situations in which such monitoring might be justified are where there are grounds for suspecting criminal activity or equivalent malpractice, and that notifying individuals about the monitoring would prejudice its prevention or detection.