Birkbeck
UNIVERSITY OF LONDON

Information Services

Birkbeck Information Security Policy

Supporting Policy 4: Birkbeck IT Facilities Monitoring and Access Policy

Approved by Strategic Planning Committee

4 July 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

Birkbeck respects the privacy of its community. From time to time, individual users' accounts and their use of IT facilities might be monitored, but such monitoring will only be undertaken with a high level of justification. For the avoidance of doubt, in this document and associated forms, *monitoring* encompasses access to data as well as user activity. Appropriate controlled conditions will be ensured when such monitoring is carried out and any monitoring of specific individuals will only be undertaken in exceptional circumstances.

2. Purpose

The purpose of this policy is to set out the rules for any monitoring and to ensure the protection of privacy of all users. The aim of this policy is to clarify the degree of privacy users can expect when using the College IT systems and to ensure those carrying out such activity are properly protected and authorised to do so.

This policy also defines the approach taken when access to an individual user's account (and any data within it) is required in their absence.

3. Scope

This policy is applicable to all users of Birkbeck's IT systems, including all staff, students and other relevant parties including members, tenants, visitors, external partners and contractors.

It covers, but is not limited to, any systems or data attached to the Birkbeck's IT facilities, any systems supplied by Birkbeck, any communications sent to or from Birkbeck and any data - which is owned either by the College or the Birkbeck-held systems external to Birkbeck's network.

4. Monitoring of the use of IT facilities at Birkbeck

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.

Users agree that authorised persons from the organisation may access all such data, and that access by such persons will not be considered a violation of the users' privacy.

The organisation may use specialised tools for the purpose of identifying and blocking forbidden methods of communication and filtering forbidden content.

The College monitors and records the use of its IT facilities for the purposes of:

- effective and efficient planning and operation of the IT facilities;

- detecting, investigating or preventing misuse of the facilities or breaches of the College’s regulations;
- investigation of alleged misconduct.

Authorisation and/or access may be withheld, withdrawn, restricted or suspended at any time by IT Services or a relevant department in the interests of safety or security, for the purposes of maintaining services, in the interests of preventing or investigating possible abuse or misuse, or other infringement of this policy.

The College will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

5. Conditions for monitoring

5.1 Routine automated scanning

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. Mail that appears to be malicious is quarantined or blocked depending on severity.

5.2 Specific monitoring

Requests for the monitoring of an individual's use of IT and telecommunication services or the content of such communications require the explicit authorisation from the appropriate member of the College's Senior Management Team (as defined below).

Following such approval, the monitoring will be undertaken by designated staff within ITS acting, for operational reasons, under the direction of the Chief Information Officer or Head of Information Security as appropriate.

Staff carrying out monitoring are required to observe the strictest confidentially when undertaking these activities and they will record or monitor only to the extent necessary in each case and within the scope of their authorisation.

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 law distinguishes between monitoring for operational and policy reasons. However, both classes of activity must be authorised. Note that authorisation mechanisms are different in the two cases.

5.2.1 Operational monitoring

Routine monitoring for operational reasons (see Monitoring form M01) may be authorised through staff job descriptions or by written authorisation from one of the following (or their deputies) as appropriate:

- the Chief Information Officer;
- the Head of Information Security (in pursuance of security issues);
- the Professional Services Director or Executive Dean (in relation to systems under his/her authority).

5.2.2 Monitoring for policy and legal compliance

Monitoring or access to stored material to investigate policy (or legal) compliance (see form M01) may only be carried out with written authorisation from one of the following (or their line manager or deputies) as appropriate:

- the College Secretary
- the Director of Human Resources (in pursuance of staff disciplinary matters)
- the Academic Registrar (in pursuance of student disciplinary matters)
- the Head of Information Security (in pursuance of security issues)

In addition, for all specific monitoring, written authorisation must be obtained from the Head of Information Security and the Birkbeck Data Protection Officer. Note that authorisation covers an individual act of monitoring and only for the purposes and scope indicated on the authorisation form.

6. Unauthorised monitoring

You must not attempt to carry out any monitoring of the use of the IT facilities other than as described in this policy.

7. Access to staff IT account in the absence of the account holder for business continuity purposes

The College reserves the right to access a current or former staff member’s IT account in the unexpected or prolonged absence (e.g. due to sickness), or following their departure from the organisation 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 individual. However, where impracticable, inappropriate or if the individual is not readily contactable, then the College reserves the right to access the account for business related information.

Requests for access to a staff member’s account should be made using and appropriately authorised form M02 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 (including an explanation of why a delay/lack of access would be detrimental to the College's interests).

Access to an account may only be provided with written authorisation from one of the following (or their line manager or deputies) as appropriate:

- Director of Professional Services or Executive Dean as appropriate.

In addition, for all access requests, written authorisation must be obtained from the Birkbeck Data Protection Officer. Note that authorisation only covers the purposes and scope indicated on the authorisation form.

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.

8. Unauthorised Monitoring

You must not attempt to monitor the use of IT without the appropriate authorisation. This would include these activities:

- monitoring of network traffic;
- network and/or device discovery;
- WiFi traffic capture;
- installation of key-logging or screen-grabbing software that may affect users other than yourself;
- attempting to access system logs or servers or network equipment.

Where IT is itself the subject of study or research, special arrangements will have been made, and you should contact your course leader / research supervisor for more information.

9. Oversight

The Birkbeck Data Protection Officer will report regularly to the IT Security and Governance Group on the volumes and sources of monitoring and access requests. This will inform any necessary changes in procedures.

10. Version Control

Version	**Date**	**Author**	**Description of change**
0.1	26 April 2021	Abu Hossain	First draft

0.2	29 April 2021	Reviewed by Abu Hossain	Added the context section.
0.3	5 May 2021	Reviewed by Abu Hossain	Moved content from other policies to this policy
0.4	14 February 2022	Marion Rosenberg	Minor edits for clarity and consistency. Added details about appropriate authorisation requirements.
0.5	12 April 2022	Marion Rosenberg and James Smith	Revisions to ensure consistency and clarity.