Birkbeck
UNIVERSITY OF LONDON

Information Services

Birkbeck Information Security Policy
Supporting Policy 2: Birkbeck Acceptable Use 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

This policy has been produced to ensure that users of the IT services and facilities provided by Birkbeck, University of London are aware of the conduct that is required of them. The aim of these regulations is to help ensure that Birkbeck's IT facilities can be used safely, lawfully and equitably.

All users are advised that monitoring of individual usage may occur to ensure compliance with this policy, and all allegations of misuse will be thoroughly investigated, including the examination of web browsing history, files and email in a user's file store.

2. Scope

This policy applies to anyone using the IT facilities (e.g. hardware, software, data, network access, third party services, online services, IT credentials) provided or arranged by the College. The scope of the policy includes, but not limited to the following:

- **Governance**

Users must not break the law. They must abide by this policy and others within the Birkbeck IT Regulations. They also must observe the policies of any third parties whose facilities they access.

- **Identity**
  Users must not allow anyone else to use their Birkbeck IT credentials. They also must not disguise their online identity and attempt to obtain/use anyone else's identity.

- **Infrastructure**
  Users must not put Birkbeck's IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.

- **Information**
  Users must safeguard all data, including personal/business data and respect other people's information. They also must not abuse copyright material.

- **Behaviour**
  Users must not waste IT resources, interfere with others' legitimate use or behave towards others in a way that would not be acceptable in the physical world.

3. Policy Statement

3.1 Governance

- When using IT facilities, you remain subject to the same laws and regulations as in the physical world. It is expected that your conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

- When accessing services from another jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service.

- You are bound by the policies within the Birkbeck IT Regulations when using the IT facilities.

- You must abide by the policies applicable to any other organisation whose services you access such as Janet and eduroam. When using services via eduroam, you are subject to both the regulations of Birkbeck and the institution where you are accessing services. If you are using Birkbeck IT credentials to access third party websites, you must then abide by both Birkbeck and third party regulations. Some software licences procured by Birkbeck will set out obligations for the user - these should be adhered to. If you use any software or resources covered by another agreement, such as Chest, you are deemed to have accepted the User Acknowledgement of Third-Party Rights. Links to the relevant policies of the external organisations are available on the Birkbeck IT Regulations page.

- Breach of any applicable law or third-party regulation will be regarded as a breach of Birkbeck IT Regulations.

3.2 Authority

This policy is approved by Strategic Planning Committee.

The Chief Information Officer who is responsible for its interpretation and enforcement, and may also delegate such authority to other people.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of this policy. If you feel that any such instructions are unreasonable or are not in support of this policy, you may appeal to the Chief Information Officer.

3.3 Intended Use

The IT facilities are provided for use in furtherance of the mission of Birkbeck, for example, to support a course of study, research or in connection with your employment by the institution.

Use of these facilities for non-commercial personal activities (provided that it does not infringe Birkbeck IT Regulations, software licences, and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point. Private use of IT facilities must not breach any other Regulation, for example data protection. Users must ensure that their private use does not put any personal or corporate information at risk. They must comply with the appropriate data protection regulation and Birkbeck's internal policies. If the private use of IT facilities causes the College any reputational damage, it may also be treated as a breach of this policy.

Use of the IT facilities for non-institutional commercial purposes or for personal gain requires the explicit approval of the Chief Information Officer.

Use of certain licences is only permitted for academic use. If in doubt, please check the appropriate licence agreement.

3.4 Identity

You must take all reasonable precautions to safeguard any IT credentials (for example a username and password, PIN, email address, smart card or other identity hardware) issued to you. You must not allow anyone else to use your IT credentials. No one has the authority to ask you for your password, and you must not disclose it to anyone. You must respect the confidentiality, integrity and security of all personal and corporate data held and processed on Birkbeck's systems.

You must not attempt to obtain or use anyone else's credentials.

You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

3.5 Infrastructure

You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval from IT Services:

- damaging, reconfiguring or moving equipment;
- loading software on to the College equipment other than in approved circumstances;
- reconfiguring or connecting equipment to the network other than by approved methods;
- setting up servers or services on the network;
- deliberately or recklessly introducing malware;
- attempting to disrupt or circumvent IT security measures.

3.6 Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe Birkbeck's Data Protection Policy, Birkbeck Information Security Policy and other relevant policies. Links to these policies are available on the Birkbeck IT Regulations page.

You must not infringe copyright or break the terms of licences for software or other material. You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the Director of IT.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory.

3.7 Behaviour

Real world standards of behaviour apply online and on social networking platforms, such as Facebook and Twitter.

You must not cause needless offence, concern or annoyance to others. You should also adhere to Birkbeck's principles for the use of social media, a link to which is available on the Birkbeck IT Regulations page.

You must not send spam (unsolicited bulk email).

You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables.

You must not use the IT facilities in a way that interferes with others' valid use of them.

3.8 Monitoring

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

3.9 Infringement

You must inform the Head of Information Security (infosec@bbk.ac.uk) if you become aware of any actual or suspected infringement of this policy.

Where infringements are not reported in a timely manner, result in serious harm to systems, services, reputation, or result in significant costs to the College, then they may result in sanctions under the College's disciplinary processes. Penalties may include withdrawal of services and/or fines. Offending material will be taken down.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

In extreme circumstances, the College reserves the right to recover from you any costs incurred as a result of your infringement.

4. Version Control

Version	Date	Author	Comments
0.1	27 October 2020	Abu Hossain	First draft. Content rearranged from policy previously known as Birkbeck Computing Regulations.
0.2	2 March 2021	Reviewed by James Smith	Suggested updates regarding the monitoring section.
0.3	29 April 2021	Reviewed by Abu Hossain	Moved the monitoring sections from different policies including this policy and created a separate policy. Added the context section.
0.4	14 February 2022	Marion Rosenberg	Minor changes for consistency and accuracy
0.5	28 March 2022	Reviewed by Marion Rosenberg and James Smith	Updates prior to SPC circulation.