Birkbeck
UNIVERSITY OF LONDON

Information Services

Birkbeck Information Security 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.

This policy statement does not form part of a formal contract of employment with Birkbeck, but it is a condition of employment that employees will abide by the regulations and policies made by the College from time to time. Likewise, these are an integral part of the regulations for students.

1. Introduction

Birkbeck's IT systems underpin all Birkbeck activities, and are essential to its teaching, research and administrative functions. The College recognises the need for its members, employees and visitors to have access to the information they require in order to carry out their work. The College also recognises the role of information security in enabling this. Security of information must therefore be an integral part of Birkbeck's management structure in order to maintain continuity of its business, regulatory compliance and compliance to the College's own policies.

2. Principles of Information Security

The fundamental principles of Information Security are the appropriate protection of the confidentiality, integrity and availability of information. Together, they are called the CIA Triad.
Confidentiality: To ensure that Information is only accessible to people who should have access to it
Integrity: To ensure that Information has not been tampered or damaged
Availability: To ensure that information is accessible by the authorised users when they need it

3. Purpose

This policy defines the framework within which information security will be managed across Birkbeck and demonstrates management direction and support for information security throughout the College.

The objectives of this policy are to:

- ensure that Birkbeck's IT facilities and information assets are adequately protected against loss, misuse or abuse
- create awareness across the College that appropriate security measures must be implemented to safeguard the IT facilities and data
- ensure that all system administrators and users understand their own responsibilities for protecting the IT facilities and data
- ensure the high availability of IT systems and to facilitate the rapid tracking down and resolution of any IT problems by IT Services and others
- protect Birkbeck's reputation
- help preserve the integrity and privacy of users' information; and
- reduce interruptions to the service, and unnecessary calls on support staff.

4. Scope

This policy applies to all Birkbeck staff and students and other relevant, authorised, 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.

5. Managing information security

5.1. Information security requirements

This Policy must be compliant with legal and regulatory requirements relevant to the organisation in the field of information security, as well as with contractual obligations.

5.2. Responsibilities

Responsibilities for Information Security generally:

- Everyone who makes use of the College's information assets is responsible for protecting them. Individuals will, at all times, act in a responsible and professional way in this respect.

- The Chief Information Officer has overall responsibility for the definition of appropriate IT policy and management of central services in accordance with those policies.

- The IT Security and Governance Group (ITSAG) is responsible for defining an information security policy and for ensuring it is discharged to all academic and administrative departments and divisions through the respective department leadership. The policy will normally apply to associated bodies, including the Students' Union and College-owned companies.

- Heads of both academic and professional services departments are required to implement this policy in respect of systems operated by their departments and are responsible for ensuring that staff, students and other persons authorised to use those systems are aware of and comply with them and associated codes of practice.

- The IT Security and Governance Group advises the SPC on matters related to compliance with this policy, and is responsible for regularly reviewing it for completeness, effectiveness and usability. In collaboration with Birkbeck Information Security, it will from time to time make available supplementary procedures and codes of practice, and promote them throughout the College; once approved by ITSAG these will also be binding on departments.

- Birkbeck Information Security will also arrange for analysis of security assessments received from departments and divisions, and report on these to the ITSAG.

- Staff with supervisory responsibility are required to coach and encourage best practice among their supervised staff or students. It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff for which they are responsible are made fully aware of the policy. Line managers also must ensure that staff members are given appropriate support and resources to comply with this policy.

- It is the responsibility of each individual to ensure their understanding of, and compliance with, this policy and any associated procedures or codes of practice.

- Further details are available in the Information Security Roles and Responsibilities Policy, a link to which can be found on the Birkbeck IT Regulations page.

7. Governance

You are bound by the Birkbeck IT Regulations, which means you must adhere to all the policies, guidelines and other internal and external documents that make up Birkbeck IT Regulations.

Supporting procedures and codes of practice amplifying this policy are published with it and are available on the College website. Staff, students and any third parties authorised to access the College's IT services, are required to familiarise themselves with these and to work in accordance with them. Guidance notes will also be published to facilitate this.

8. Awareness of this policy and IT Regulations

Birkbeck is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the college. It is the college's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance. Therefore, it is the responsibility of everyone in scope to familiarise themselves with the Birkbeck IT Regulations.

All staff and students will be made aware of this policy and the Birkbeck IT Regulations (by HR or Registry as appropriate. Existing staff and students of the College, authorised third parties and contractors given access to the College IT facilities will be advised of the existence of this policy statement and the availability of the associated procedures, codes of practice and guidelines which are published on the College website. Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

Individuals requiring education about any aspects of the policy should discuss their needs with the Head of Information Security, who will, in the first instance, be responsible for interpretation and clarification of the information security policy.

9. Information Risk Management within departments

Appropriate management of information risks is vital for ensuring information security. To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches. Without proper assessment of the value of information assets, and the consequences (financial and otherwise) of loss of data or disruption to service, efforts to improve security are likely to be poorly targeted and ineffective. Similarly, periodic review is necessary to take into account changes to technology, legislation, business requirements and priorities; and security arrangements should be revised accordingly.

Heads of Departments/Executive Deans should establish effective contingency plans appropriate to the outcome of any risk assessment. In addition, they are required to carry out periodic assessments (at least once every five years) of the security arrangements for their information management systems and submit a report on this to the ITSAG.

10. Legal Obligation

Your behaviour is subject to the laws of the land, even those that are not apparently related to IT such as the laws on fraud, theft and harassment.

Of particular importance is the Computer Misuse Act 1990 and the Data Protection Act 2018. This policy satisfies the Data Protection Act's requirement for a formal statement of the College's security arrangements for personal data. The requirement for compliance devolves to all users defined above, who may be held personally responsible for any breach of the legislation.

There are many items of legislation that are particularly relevant to the use of IT. Links to the details of these laws are available on the Birkbeck IT Regulations page.

Full texts of relevant legislation are available at https://www.legislation.gov.uk/.

11. Reporting a (potential) breach of Security

IT Services will monitor network activity, receive reports from Birkbeck Information Security and other security agencies, and take action/make recommendations consistent with maintaining the security of College IT and information assets.

Any individual suspecting that there has been, or is likely to be, a breach of information security should inform Birkbeck Information Security (infosec@bbk.ac.uk) immediately. Birkbeck Information Security will advise the College on what steps should be taken to avoid incidents or minimise their impact, and identify action plans to reduce the likelihood of recurrence.

In the event of a suspected or actual breach of security, Birkbeck Information Security may, after consultation with the relevant system owner/Head of Department, require that any unsafe systems, user/login names, data and/or programs be removed or made inaccessible.

Where a breach of security relates to personal information, there may be an infringement of the Data Protection Act 2018 which could lead to civil or criminal proceedings. It is vital, therefore, that users of the College's information systems comply, not only with this policy, but also with Birkbeck's Data Protection Policy and associated codes of practice, details of which may be found on the College website.

12. Implementation of the policy and sanctions

Failure to comply with this policy that occurs because of deliberate, malicious or negligent behaviour, may result in disciplinary action.

Any breach of this policy should be reported to IT Services, a link to their contact details is available on the Birkbeck IT Regulations page. IT Management team will ensure that appropriate action is taken.

In the event of a suspected or actual breach of security, IT Services may remove any affected device from the network.

Failure of an individual to comply with this policy may lead to the instigation of the relevant disciplinary procedures for students and staff. This may result in withdrawal of access to College's IT facilities and could result in suspension of students or dismissal of staff. In the event of a serious infringement the College may also decide to institute legal proceedings under civil or criminal law.

13. Version Control

Version	Date	Author	Description of change
0.1	27 October 2020	Abu Hossain	First draft.
0.2	3 March 2021	Reviewed by James Smith	Suggested improvement about the policy objectives
0.3	22 April 2021	Reviewed by Abu Hossain	Added policy statements about the Information Security Management System. Added objective of the policy.
0.4	29 April 2021	Reviewed by Abu Hossain	Added the context section. Removed some duplicate information and put references to the Birkbeck IT Regulations landing page
0.5	3 February 2022	Reviewed by Marion Rosenberg	Clarified status of document as policy. Clarified responsibilities for information security and various changes for accuracy, completeness, clarity and readability.
0.5	28 March 2022	Reviewed by Marion Rosenberg and James Smith	Updates prior to SPC circulation.