Information Services

Birkbeck Information Security Policy

Guidelines 1: Birkbeck Acceptable Use Guidelines

Approved by Strategic Planning Committee

4 July 2022

0. Context

This guidance 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 guidance expands on the principles set out in the Birkbeck Acceptable Use Policy, a link to which can be found on the Birkbeck IT Regulations page. It gives many examples of specific situations and is intended to help you relate your everyday use of the IT facilities to the dos and don'ts in the Acceptable Use Policy.

Where a list of examples is given, these are just some of the most common instances, and the list is not intended to be exhaustive.

Where the terms similar to Authority, Authorised, Approved or Approval appear, they refer to authority or approval originating from the person or body identified in the Authority section below, or anyone with authority delegated to them by that person or body.

2. Definitions

2.1 User

User means anyone using Birkbeck's IT facilities. This means more than students and staff. It could include, for example:

- visitors to the Birkbeck website, and people accessing the institution's online services from off campus;
- external partners, contractor and agents based on site and using the Birkbeck network, or offsite and accessing the institution's systems;
- tenants of the institution using the College's computers, servers or network;
- visitors using the institution's WiFi;
- students and staff from other institutions logging on using eduroam.

2.2 IT Facilities

The term IT Facilities include:

- IT hardware that Birkbeck provides, such as PCs, laptops, tablets, smart phones and printers;
- Software that Birkbeck provides, such as operating systems, office application software, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example special deals for students on commercial application packages;
- Data that Birkbeck provides or arranges access to. This might include online journals, data sets or citation databases;
- Access to the network provided or arranged by Birkbeck. This would cover, for example, on-campus WiFi, connectivity to the internet from College PCs;
- Online services arranged by the institution or any of the JISC online resources;
- IT credentials, such as the use of Birkbeck log-in, or any other token (email address, smartcard, dongle) issued by the College to identify yourself when using IT facilities. For example, you may be able to use drop-in facilities or WiFi connectivity at other institutions using your usual username and password through the eduroam system.

3. Governance

It is helpful to remember that using IT has consequences in the physical world.

Your use of IT is governed by IT-specific laws and regulations (such as Birkbeck IT Regulations), but it is also subject to general laws and regulations such as Birkbeck's general policies.

3.1 Domestic Law

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.

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.

So, for example, you may not:

- create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety;
- create or transmit material with the intent to defraud;
- create or transmit defamatory material;
- create or transmit material such that this infringes the copyright of another person or organisation;
- create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe;
- deliberately (and without authorisation) access networked facilities or services.

Overviews of law relating to IT use is available from Jisc, a link to which can be found on the Birkbeck IT Regulations page.

3.2 Foreign Law

If you are using services that are hosted in a different part of the world, you may also be subject to their laws. It can be difficult to know where any particular service is hosted from, and what the applicable laws are in that locality.

In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

3.3 General Institutional Regulations

You should already be familiar with Birkbeck's regulations and policies. Additional regulations can be found via the College's website, links are available on the Birkbeck IT Regulations page.

3.4 Third Party Regulations

If you use Birkbeck's IT facilities to access third party services or resources, you are bound by the regulations associated with that service or resource. The association can be through something as simple as using your institutional username and password.

Very often, these regulations will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it. Examples of this would be:

- **Using Janet, the IT network that connects all UK higher education and research institutions together and to the Internet**
  When connecting to any site outside Birkbeck you will be using Janet, and subject to the Janet Acceptable Use Policy, the Janet Security Policy and the Janet Network Connection Policy. Links to these policies are available on the Birkbeck IT Regulations page.
- Using Chest agreements
  A Chest Agreement is a contract between a supplier of commercially available software or online resources to licence their product(s) to the education and research communities in the UK. Chest agreements have certain restrictions that may be summarised as follows:
    - non-academic use is not permitted
    - copyright must be respected
    - privileges granted under Chest agreements must not be passed on to third parties
    - users must accept the User Acknowledgement of Third Party Rights.

  Links relevant to Chest agreements are available on the Birkbeck IT Regulations page.
- **Licence agreements**
  There will be instances where the College has provided you with a piece of software or a resource. Users shall only use software and other resources in compliance with all applicable licences, terms and conditions.

4. Authority

The Birkbeck Acceptable Use Policy is issued under the authority of the Strategic Planning Committee. The Chief Information Officer is responsible for its interpretation and enforcement, and may also delegate such authority to other people.

Authority to use the College's IT facilities is granted by a variety of means. For example,

- the issue of a username and password or other IT credentials
- the explicit granting of access rights to a specific system or resource
- the provision of a facility in an obviously open access setting, such as an Institutional website; a self-service kiosk in a public area; or an open WiFi network on the campus.

If you have any doubt whether or not you have the authority to use an IT facility you should seek further advice from IT Services. A link to their contact details is available on the Birkbeck IT Regulations page.

Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act 1990.

5. Intended Use

Birkbeck's IT facilities, and the Janet network that connects institutions together and to the Internet, are funded by the tax-paying public. They have a right to know that the facilities are being used for the purposes for which they are intended.

5.1 Use for Purposes in Furtherance of Institution's Mission

The IT facilities are provided for use in furtherance of Birkbeck's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the institution, or the administration necessary to support all of the above.

5.2 Personal Use

You may currently use the IT facilities for personal use provided that it does not breach Birkbeck IT Regulations and that it does not prevent or interfere with other people using the facilities for valid purposes (for example using a PC to update your social media page when others are waiting to complete their assignments. However, this is a concession and can be withdrawn at any time. Employees using the IT facilities for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity.

5.3 Commercial Use and Personal Gain

Use of IT facilities for non-institutional commercial purposes or for personal gain, such as running a club or society, requires the explicit approval of the Chief Information Officer. The provider of the service may require a fee or a share of the income for this type of use. For more information, contact the Chief Information Officer.

Even with such approval, the use of licences under the Chest agreements for anything other than teaching, studying or research, administration or management purposes is prohibited, and you must ensure that licences allowing commercial use are in place.

6. Identity

Many of the IT services provided or arranged by the College require you to identify yourself so that the service knows that you are entitled to use it. This is most commonly done by providing you with a username and password, but other forms of IT credentials may be used, such as an email address, a smart card or some other form of security device.

6.1 Protect Identity

You must take all reasonable precautions to safeguard any IT credentials issued to you. For example:

- You must change passwords when first issued and at regular intervals as instructed. Do not use obvious passwords, and do not record them where there is any likelihood of someone else finding them. Do not use the same password as you do for personal (i.e. non-institutional) accounts. Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem.
- If you think someone else has found out what your password is, change it immediately and report the matter to the IT Services. A link to their contact details is available on the Birkbeck IT Regulations page.
- Do not use your username and password to log in to web sites or services you do not recognise, and do not log in to web sites that are not showing the padlock symbol.
- Do not leave logged in computers unattended, and log out properly when you are finished.
- Do not allow anyone else to use your smartcard or other security hardware. Take care not to lose them, and if you do, report the matter to IT Services immediately.

6.2 Impersonation

Never use someone else's IT credentials or attempt to disguise or hide your real identity when using the institution's IT facilities. However, it is acceptable not to reveal your identity if the system or service clearly allows anonymous use (such as a public-facing website).

6.3 Attempt to Compromise Others' Identities

You must not attempt to usurp, borrow, corrupt or destroy someone else's IT credentials.

7. Infrastructure

The IT infrastructure is all the underlying stuff that makes IT function. It includes servers, the network, PCs, printers, operating systems, databases and a whole host of other hardware and software that has to be set up correctly to ensure the reliable, efficient and secure delivery of IT services. You must not do anything to jeopardise the infrastructure.

7.1 Physical Damage or Risk of Damage

Do not damage, or do anything to risk physically damaging the infrastructure, such as being careless with food or drink at a PC.

7.2 Reconfiguration

Do not attempt to change the setup of the infrastructure without authorisation, such as changing the network point that a PC is plugged in to, connecting devices to the network (except of course for WiFi or Ethernet networks specifically provided for this purpose or altering the configuration of the institution’s PCs. Unless you have been authorised, you must not add software to or remove software from PCs. Do not move equipment without authority.

7.3 Network Extension

You must not extend the wired or WiFi network without authorisation. Such activities, which may involve the use of routers, repeaters, hubs or WiFi access points, can disrupt the network and are likely to be in breach of the Janet Security Policy, a link to which can be found on the Birkbeck IT Regulations page.

7.4 Setting up Servers

You must not set up any hardware or software that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, internet relay chat servers or websites.

7.5 Introducing Malware

You must take all reasonable steps to avoid introducing malware to the infrastructure. The term malware covers many things such as viruses, worms and Trojans, but is basically any software used to disrupt computer operation or subvert security. It is usually spread by visiting websites of a dubious nature, downloading files from untrusted sources, opening email attachments from people you do not know, or inserting media that have been created on compromised computers.

If you avoid these types of behaviour, keep your anti-virus software up to date and switched on, and run scans of your computer on a regular basis, you should not fall foul of this problem.

7.6 Subverting Security Measures

Birkbeck has taken measures to safeguard the security of its IT infrastructure, including things such as anti-virus software, firewalls, spam filters and so on. You must not attempt to subvert or circumvent these measures in any way.

8. Information

8.1 Personal, Sensitive and Confidential Information

During the course of their work or studies, staff and students (particularly research students may handle information that comes under the Data Protection Act 2018, or is sensitive or confidential in some other way. For the rest of this section, these will be grouped together as protected information.

Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. The institution has policies on Data Protection and Information Management, a link to which can be found on the Birkbeck IT Regulations page. If your role is likely to involve handling protected information, you must make yourself familiar with and abide by these policies.

Additional guidance on the provisions of the Data Protection Act 2018 and how Birkbeck ensures compliance with it is available at the Privacy page of the College website. A link to which can be found on the Birkbeck IT Regulations page.

8.1.1 Transmission of Protected Information

When sending protected information electronically, you must use a method with appropriate security. Email is not inherently secure. Advice about how to send protected information electronically is available via the College IT Services, a link to their contact details is available on the Birkbeck IT Regulations page.

8.1.2 Removable Media and Mobile Devices

Protected information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs or mobile devices (laptops, tablet or smart phones unless it is encrypted, and the encryption key kept securely.

If protected information is sent using removable media, you must use a secure, tracked service so that you know it has arrived safely. To get more advice and learn about the policies and guidelines on the use of removable media and mobile devices for protected information, please refer to the relevant sections at the Birkbeck IT Regulations page.

Additional information is available from the College IT Services. A link to their contact details is available on the Birkbeck IT Regulations page.

8.1.3 Remote Working

If you access protected information from off campus, you must make sure you are using an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service. You must also be careful to avoid working in public locations where your screen can be seen.

8.1.4 Personal or Public Devices and Cloud Services

Even if you are using approved connection methods, devices that are not fully managed by Birkbeck cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. You should not therefore use such devices to access, transmit or store protected information. Advice on the use of personal devices to access institutional services can be made available via the College IT Services. A link to their contact details is available on the Birkbeck IT Regulations page.

Do not store protected information in personal cloud services such as Dropbox unless securely encrypted first.

8.1.5 Copyright Information

Almost all published works are protected by copyright. If you are going to use material (images, text, music, software, the onus is on you to ensure that you use it within copyright law. This is a complex area, and guidance is available from the Birkbeck Library, a link to which can be found on the Birkbeck IT Regulations page. The key point to remember is that the fact that you can see something on the web, download it or otherwise access it does not mean that you can do what you want with it.

8.2 Others' Information

You must not attempt to access, delete, modify or disclose restricted information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you have approval from the Copyright Owner.

Where information has been produced in the course of employment by Birkbeck and the person who created or manages it is unavailable, the responsible line manager may give permission for it to be retrieved for work purposes. In doing so, care must be taken not to retrieve any private information in the account, nor to compromise the security of the account concerned.

Private information may only be accessed by someone other than the owner under very specific circumstances governed by institutional and/or legal processes.

8.3 Inappropriate Material

Birkbeck has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The College reserves the right to block or monitor access to such material.

Universities UK has produced guidance on handling sensitive research materials, a link to which can be found on the Birkbeck IT Regulations page. There is also an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law.

8.4 Publishing Information

Publishing means the act of making information available to the general public. This includes through websites, social networks and news feeds. Whilst Birkbeck generally encourages publication, there are some general guidelines you should adhere to.

8.4.1 Representing the Institution

You must not make statements that purport to represent Birkbeck without the approval of the College Secretary or the Director of External Relations.

8.4.2 Publishing for Others

You must not publish information on behalf of third parties using the institution's IT facilities without the approval of the College Secretary or the Director of External Relations.

9. Behaviour

The way you behave when using IT should be no different to how you would behave under other circumstances. Abusive, inconsiderate or discriminatory behaviour is unacceptable.

9.1 Conduct online and on social media

Birkbeck's policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures. Please refer to Birkbeck's social media guidelines for more information, a link to which can be found on the Birkbeck IT Regulations page.

9.2 Spam

You must not send unsolicited bulk emails or chain emails other than in specific circumstances. For further advice please contact the College IT Services. A link to their contact details is available on the Birkbeck IT Regulations page.

9.3 Offensive Material

You must not create, store, exchange, display, print or circulate offensive material in any form or medium (including abusive electronic mail and pornographic material.

9.4 Denying Others Access

If you are using shared IT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them.

9.5 Disturbing Others

When using shared spaces, remember that others have a right work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area, do not obstruct passageways and be sensitive to what others around you might find offensive.

9.6 Vacating booked workstation rooms promptly

When using open access facilities which have booked for a teaching session, you must vacate the rooms promptly when requested to do so by the lecturer. Please refer to the guidelines for the acceptable use of workstation rooms, a link to which can be found on the Birkbeck IT Regulations page.

9.7 Excessive Consumption of Bandwidth / Resources

Use resources wisely. Do not consume excessive bandwidth by uploading or downloading more material (particularly video than is necessary. Do not waste paper by printing more than is needed, or by printing single-sided when double-sided would do. Do not waste electricity by leaving equipment needlessly switched on.

10. Monitoring

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.

11. Infringement

11.1 Disciplinary Process and Sanctions

Breaches of the Acceptable Use Policy and other Birkbeck IT Regulations will be handled by the College's disciplinary processes. This could have a bearing on your future studies or employment with the institution and beyond. Sanctions may be imposed if the disciplinary process finds that you have indeed breached the regulations, for example, imposition of restrictions on your use of IT facilities; removal of services; withdrawal of offending material; fines and recovery of any costs incurred by the College as a result of the breach.

11.2 Reporting to Other Authorities

If the institution believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

11.3 Reporting to Other Organisations

If the institution believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

11.4 Report Infringements

If you become aware of an infringement of these regulations, you must report the matter to the relevant authorities.

12. Version Control

Version	**Date**	**Author**	**Description of change**
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. Removed some duplicate information and put references to the Birkbeck IT Regulations landing page. Added the context section.
0.4	14 February 2022	Marion Rosenberg	Minor edits for clarity and consistency.