Information Services

Birkbeck Information Security Policy

Supporting Policy 5: Birkbeck Mobile and Remote Device 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

It is recognised that the use of mobile devices and equipment at home and other locations is commonplace, useful, and growing. It is also recognised that there are circumstances where data needs to be moved using portable media. However, there is a risk surrounding the storage of data held on mobile or remote devices, which may not be secure if care is not taken.

2. Purpose

The purpose of this policy is to remind those handling data of their responsibilities, highlight possible risks, and provide links to guidance to ensure that information is kept secure from unauthorised use and protected from loss or corruption.

3. Scope

This policy applies to anyone using a mobile device to access the College IT facilities and data. As it is unlikely that any such device would not contain personal data (as defined by the Data Protection Act 2018), this policy will be deemed to apply to all devices used for handling work or study data.

4. Responsibilities of users

All users must adhere to Birkbeck IT Regulations to fulfil their information security responsibilities. In addition to that, all staff are responsible for safeguarding the security of College data and, as such, need to be aware of this policy and guidelines.

The type of activities relevant for the security of data could be any or all of the following:

- Storing of documents, spreadsheets, images on mobile devices or equipment at home, including synchronisation with cloud services
- Sending and reading emails and email attachments
- Storing passwords, with or without username
- Storing contact details including names, addresses, phone numbers, email address

The security of data needs to be considered for all types of remote, portable or mobile storage, and can include but is not limited to USB sticks or memory sticks, memory pens, USB flash drives, MP3 Players, mobile phones, smart phones, External Hard Drives, CD Discs, SD cards and similar, DVD Discs, tapes, laptops, tablets, PDAs, home PCs, and cloud services.

5. Research data

It should be noted that there are related considerations surrounding data management and security of research data. These may be a result of possible external pressures or stipulations, including: the possible need to adhere to principles within ISO 27001 (Information Security Management); requirement for safe rooms; and in general the need to comply with Research Council funding requirements for the security and protection of information utilised for specific research projects. In such cases an individual risk assessment should be undertaken.

6. BYOD

BYOD (or Bring Your Own Device) is a commonly used term for provision of services via personal devices. This is supported at Birkbeck via the eduroam service for providing access to internet services. Such devices are treated as any other internet connected unmanaged device, and users should take the same precautions in protecting data.

7. Data classification

The data should be classified by the data owner, and consideration should be given to whether it needs to be subject to additional controls. The most obvious reasons why data may need to be classified as confidential are:

- personal data, which is subject to the Data Protection Act 2018
- data which could cause reputational or financial damage to Birkbeck if lost.

A separate policy and guidelines will be created, but please consult Birkbeck Information Security or Data Protection for advice in the meantime.

8. Data portability

Consider whether data needs to be portable. Best practice remains that data should normally be held on central servers or cloud services provided by Birkbeck IT Services. Access to these data storage facilities at Birkbeck or via secure remote access methods reduces risk and assists with the secure management of data. Using these services requires access to the internet, which may not always be possible, particularly when travelling. Portable media or devices should only be used where there is a clear and justifiable requirement to move data away from centrally managed servers.

9. Portable data risk management

It is extremely important to manage the risk of portable data. If the data does need to be portable, the following recommendations apply:

- All mobile devices must be encrypted.
- Any portable device or media must be labelled with name and telephone number.
- Serial numbers and descriptions must be recorded buy the user.
- Portable media or devices must not contain the only copy of data. The data must be backed up. Backups should be subject to the same precautions as primary data source.
- Portable devices should not be left unattended and logged in.
- Devices must be disposed of in such a way to remove data effectively.
- All reasonable precautions should be taken to avoid the physical theft or loss of portable devices. When travelling and not in use, the portable device should be stored securely out of sight.
- Devices in sleep mode should require re-authentication before access is permitted.
- Data must not be stored on a mobile device for any longer than needed.
- Suitable password protected encryption should be used on USB memory keys and other devices.

9. Encryption passwords

- Encryption passwords must not be the same as that for access to the device, or for other services
- Authentication must be required before access to services or data is permitted.
- Passwords should be strong; consisting of a minimum of nine characters which include a mixture of upper and lower case letters and at least one number or a combination of three words.
- Devices must be configured to timeout after a maximum of 15 minutes of inactivity and require re-authentication before access to services or data is permitted.
- Passwords should be stored using suitable protection

10. PC type devices

The following recommendations apply to PC type devices (e.g. desktop/laptops computers and Macs at home):

- Laptops must be protected with antivirus software, set to auto update.
- For laptops and similar devices, encryption must be enabled on the device.
- Strong password protection must be used to gain access to the device.
- The laptop's operating system software must be kept up to date.
- All removable media such as CD-ROMs, DVDs, memory cards and USB flash drives should be removed when not in use.
- Family members should not be given administrative access to a device holding Birkbeck data, and in general care should be taken with any access provided.

11. Phones and handheld devices

The following recommendations apply to phones and other handheld devices (e.g. tablets):

- Ensure sim and device passwords are set.
- Configure and utilise a remote wipe facility for use in the event the device is lost.
- Use the device’s built-in password protection and encryption.

12. Cloud services recommendations

The following recommendations apply to cloud services:

- Only services with adequate security and encryption policies may be used.
- Data must be password protected and/or encrypted separately to the service offering.
- Data should be located within the European Economic Area or within a region that has a decision of adequacy from the Information Commissioner’s Office.

13. Disposal and maintenance of equipment

All College equipment must be returned to IT Services or departmental support staff for secure disposal/data destruction when no longer used. Personal equipment can be disposed of via ITS.

Equipment repairs must be undertaken with companies under a contractual obligation to maintain data security.

14. Version Control

Version	Date	Author	Comments
1.0	March 2016	Reviewed	
1.1	14 October 2020	Reviewed by Abu Hossain	Content rearranged. Outdated/unavailable links removed/updated.
1.2	29 April 2021	Reviewed by Abu Hossain	Added the context section.
1.3	15 February 2022	Reviewed by Marion Rosenberg	Minor changes for clarity and consistency. Added point about device encryption as it was missing but assumed. Password requirement updated to be in line with NCSC recommendations. Section 7 will need updating when classification policy is available.