

Birkbeck, University of London

Malet Street, Bloomsbury

London WC1E 7HX

# Mobile and Remote Device Security Policy

### 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.

The purpose of this policy is to remind staff 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.

This policy is only relevant to data which is regarded as confidential or sensitive– That is defined as data which if lost would result in the exposure of personal data (so subject to the Data Protection Act) or data which could cause reputational or financial damage to Birkbeck. 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 e-mails and email attachments
* Storing Passwords, with or without username
* Storing contact details including names, addresses, phone numbers, e-mail 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.

If the data is not regarded as confidential, and there would be no impact if lost, then obviously greater freedom is available, and the data is not subject to the policy. However, common sense suggests that some of the same principles should be adhered to.

### 1.1 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.

### 1.2 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.

### 2. The policy

There are three principles:

* Classify the data to determine whether it needs to be subject to additional controls
* Consider whether the data needs to be portable.
* Manage the risk of portable data

### 2.1 Classifying the data

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

* personal data (so subject to the Data Protection Act)
* data which could cause reputational or financial damage to Birkbeck if lost.

### 2.2 Considering whether data needs to be portable

Best practice remains that data should normally be held on central servers.  Access to these servers at Birkbeck or via secure remote access methods reduces risk and assists with the secure management of data.

* ***How to 1)*** [*Using the VDI (Virtual Desktop Interface) at Birkbeck, to access a Windows 7 desktop, Birkbeck applications and filestore.*](http://www.bbk.ac.uk/its/services/RemoteAccess/vdi)
* ***How to 2)*** [*Using the Birkbeck VPN Service and central filestore to access files.*](http://www.bbk.ac.uk/its/services/RemoteAccess/vpn)

Using the services above 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.

### 2.3 Managing the risk

If the data does need to be portable, the following recommendations apply:

1. Any portable device or media must be labelled with name and telephone number.
2. Serial numbers and descriptions must be recorded
3. Portable media  or devices must not contain the only copy of data (ie take backups!). Backups should be subject to the same precautions as primary data source.
4. Portable devices should not be left unattended and logged in.
5. Devices must be disposed of in such a way to remove data effectively.
6. 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
7. Devices in sleep mode should require re-authentication before access is permitted
8. Data must not be stored on a mobile device for any longer than needed.
9. Suitable password protected encryption should be used on USB memory keys and other devices.

* ***How to 3)*** [*Using an encrypted USB key.*](http://www.bbk.ac.uk/its/help/documentation/its_documentation/securing_data/kingstonUSB)
* ***How to 4)*** Encrypting a laptop disk partition.
* ***How to 5)*** Using PGP to encrypt a file for sharing with others.
* ***How to 6)*** Using a personal device to synchronise email.

**Passwords**

1. Encryption passwords must not be the same as that for access to the device, or for other services
2. Authentication must be required before access to services or data is permitted.
3. Passwords should be strong; consisting of a minimum of six digits which include a mixture of upper and lower case letters and at least one number.
4. 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.
5. Passwords should be stored using suitable protection

* ***How to 7)*** storing passwords securely on Birkbeck Blackberry devices.

**Applying to PC type devices (eg laptops and equipment at home):**

1. Laptops must be protected with antivirus software, set to auto update.
2. For laptops and similar devices, encryption must be installed or enabled on the device.
3. Strong password protection must be used to gain access to the device.
4. The laptop's operating system software must be kept up-to-date.
5. All removable media such as CD-ROMs, DVDs, memory cards and USB flash drives should be removed when not in use.
6. 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.

**Applying to Phones**

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

* ***How to 8)*** Using remote wipe for android and ios

**Applying to cloud services**

1. Services with adequate security and encryption policies should be used for data subject to the policy.
2. Data should be password protected and/or encrypted separately to the service offering
3. Data should be located within the European Economic Area

* ***How to 9)*** Using Birkbeck gmail service to synchronise data.
* ***How to 10)*** Guide to using cloud services

**Disposal and maintenance of equipment**

1. All equipment which has been used to hold data subject to the policy should be returned to ITS or departmental support staff for disposal/data destruction. Personal equipment can be disposed of via ITS.
2. Equipment repairs must be undertaken with companies under a contractual obligation to maintain data security.

Date of last review: March 2016