Information Services

Birkbeck Information Security Policy
Supporting Policy 12: Birkbeck Data Classification and Information Handling Policy

Approved by Strategic Planning Committee

1 March 2023

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 is intended to help you protect the electronic information for which you are responsible. It applies to all types of information, such as personal data or research, teaching, audit or financial information; some or all of these may be held on personal workstations, servers, shared drives, laptops, USB keys and mobile devices.

Most of us keep a wide range of documents, images, presentations, technical specifications or software on our computers, which require differing minimum levels of protection from disclosure or damage. This policy will help you categorise your information and then think about the most appropriate ways of storing it to protect it against unauthorised access or use.

This classification relates to data for which you are responsible which may be held:

- on devices and systems under your day to day management and custodianship;
- on servers or shared drives under the management of a database or system administrator. In this case, you will need to liaise with the administrator(s) about the sensitivity of your data; for example, there might be a need to set up separate servers/partitions with different levels of protection if the same server is being used for data of widely differing sensitivities.

This document does not consider disclosure of information under legislation such as the Data Protection Act 2018 or the Freedom of Information Act 2000. Any requests under this legislation should be transferred immediately to dpo@bbk.ac.uk.

The classification considers information in terms of the degree of sensitivity rather than their purpose or format, and maps these to one of four levels of sensitivity: Public, Internal, Confidential and Highly confidential.

For portable devices such as laptops, mobile phones, tablets, PDAs and USB keys, consider the policy on mobile and remote device security and think twice about whether you need to carry files of higher sensitivity around with you when you travel.

The first step in protecting information is to focus on the risk of disclosure or loss and the resulting consequences. As risk assessment is a specialised area, this policy outlines particular types of data and indicates the appropriate classification to be used.

Note that data that could be considered anonymous, may no longer be anonymous if it is in the hands of someone who has other data, the combination of which allows re-identification. Also, certain types of data can effectively identify individuals - for example, postcode and date of birth is likely to be sufficient to enable individuals to be identified. There is detailed information on the Information Commissioner's website.

The appropriate ways of protecting your information, including storage, access and everyday handling are then presented.

2. Data classifications

The sensitivity classification levels are described below and relate to particular protection measures defined later.

1: Public

Description: Information that is published for the public and/or could be disclosed with no risk.

Examples: Information for the Internet; information already available publicly; information suitable for inclusion in publications; materials about Birkbeck that are known to be public; some Birkbeck policies and governance structure.

2: Internal

Description: Limited to Birkbeck staff and students and specific collaborators. Disclosure beyond this may result in temporary inconvenience to individual(s) or organisation(s) or minor damage to reputation that can be recovered and has a small containment cost.

Examples: Project documentation; address books; anonymised data that cannot be re-identified; aggregated datasets; organisational information that is appropriate for Birkbeck staff and students only; staff training records; some committee minutes.

3: Confidential

Description: Limited to specific named individuals. Disclosure beyond this will cause significant upset to individuals or is expected to result in containment costs and/or financial penalty.

Examples: Interview notes; disciplinary correspondence; staff salaries; exam board minutes; datasets with special category personal data; student demographic details and assessments; staff appraisals and assessments; internal and external audit reports; program code for BBK core services (some may be in category 4).

4: Highly Confidential

Description - Very rare - limited to specific named individuals having to work in a very restricted manner due to the risk of significant legal liability or severe distress/danger to individual(s) or severe damage to organisational reputation or significant loss of asset value.

Examples: Personal health data about identifiable individuals; staff bank details.

3. Data classification and handling

	1: Public	2: Internal	3: Confidential	4: Highly confidential
Classification description	Available to all	Available within Birkbeck	Named Birkbeck individuals and/or collaborators	Named individuals only under strict controls
Level of risk if disclosed in error	None	Low	Medium	High
Examples (see section 2 above for further examples)	Birkbeck website, any information within Birkbeck's publication scheme, publications, press releases	Information limited to Birkbeck, internal policies and procedures	HR data, including recruitment materials for panels only, special category personal data (as per DPA) including much of our research data.	Research data that is personally identifiable (or can be linked with other data to become identifiable) and required to be held in isolation, possibly by the body sharing the data (the data controller).
Access control	No particular requirements	Require Birkbeck log-in credentials	Require specific controls	Require specific controls

Electronic storage (fixed equipment)	No particular requirements	No special requirements on fixed equipment	Access controls and recommend encryption - 256-bit minimum	Access controls and encryption (data or device) required - 256-bit minimum
Electronic storage (mobile devices including mobile phones and tablets)	No particular requirements	Recommend to encrypt data or device - 256 bit minimum	Encrypt data or device - 256-bit minimum - or do not sync to mobile device	Must not be stored on mobile device
Electronic transmission (email)	No particular requirements	Consider recipients and limit circulation	Encryption advisable, else anonymise data - 256-bit minimum	Encrypt if absolutely necessary to email - 256-bit minimum
Electronic transmission (fax)	No particular requirements	Do test fax and require recipient to be present	Do test fax and require recipient to be present	Fax not allowed
Electronic transmission (voicemail)	No particular requirements	Take care to ensure correct recipient	Take care to ensure correct recipient and do not leave any details in voicemail	Take care to ensure correct recipient and do not leave any details in voicemail
Electronic transmission (file transfer)	No particular requirements	Use secure transfer	Use secure transfer as per data transfer agreement (create one if this does not exist)	File transfer not allowed
Paper handling (labelling)	No particular requirements	Consider labelling '2-Internal" (Birkbeck only)'	Label – '3-Confidential' and give a list of people allowed to see.	Label '4-Highly Confidential' and give list of people allowed to see.
Paper handling (printing)	No particular requirements	Collect printout ASAP	No unattended printing - collect immediately	No unattended printing - collect immediately
Paper handling (duplication)	No particular requirements	Limited duplication	Limited duplication	Very limited duplication

Paper handling (storage)	No particular requirements	Clear desk policy - out of sight when not in use	Store in secured location	Store in secured location
Paper handling (transmission - posting)	No particular requirements	Care to keep to intended audience - seal envelope	Consider secure postage.	Secure postage to named recipient only
Paper handling (data owner review)	Annual review - as per records management procedure	Annual review - as per records management procedure	Annual review - as per records management procedure	Annual review - as per records management procedure
Disposal (paper)	No particular requirements	Shred	Shred - cross-cut	Shred - cross-cut
Disposal (electronic)	No particular requirements	Secure deletion of electronic data	Secure deletion of electronic data	Physical destruction beyond ability to recover

4. Version control

Version	Date	Author	Comments
1.0	March 2022	Marion Rosenberg	
2.0	April 2022	Marion Rosenberg	With input from Avi Reisman
		Approved by	ITSAG, SPC