Guidelines 2: Birkbeck information storage options – approved by ITSAG 27 November 2023

- **Public**: Information that is published for the public and/or could be disclosed with no risk.
- **Internal**: Limited to Birkbeck staff and students and specific collaborators.
- **Confidential**: Limited to specific named individuals.
- **Highly confidential**: Limited to specific named individuals having to work in a very restricted manner.

These tables support the Birkbeck Data Classification and Information Handling Policy, which is a supporting policy of the Birkbeck Information Security Policy. You should read the Birkbeck Data Classification and Information Handling Policy for background information on data classification as this is primarily guidance on handling/storing the data **after** you have correctly classified it. Storage, in this context, relates to where there is an expectation of data persistence.

Classification	Level of risk if disclosed in error	Examples	Access control	Appropriate storage
Public	None	Birkbeck website, information within the College's publication scheme, publications or press releases.	No particular requirements	M365 Onedrive M365 Sharepoint MS Teams
Internal	Low	Information limited to Birkbeck, internal policies and procedures.	Require Birkbeck log-in credentials. Mobile devices – recommend encrypting data or device – 256-bit minimum.	M365 Onedrive M365 Sharepoint MS Teams
Confidential	Medium	HR data, including recruitment materials for panels only, special category data (as per DPA 2018).	Require specific controls. Access controls and recommend encryption - 256-bit minimum Mobile devices - encrypt data or device - 256-bit minimum - or do not sync to mobile device.	M365 Onedrive M365 Sharepoint
Highly confidential	High	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).	Require specific controls. Access controls and encryption (data or device) required - 256-bit minimum Must not be stored on mobile devices.	M365 Onedrive M365 Sharepoint Note: HR data should remain in dedicated HR systems – except for anonymised reports.

Storage system	Purpose	Public	Internal	Confidential	Highly confidential	Auto backup	Accessible to:	Data encryption	File access auditing	Remote access	Notes
M365 - Onedrive	Data storage and transfer. For personal data – used to be on N: drives.	Yes	Yes	Yes	Yes, with appropriate config	Yes	User and sysadmin	Yes	Yes	Yes	Others can be given access if have federated accounts.
M365 - Sharepoint	Data storage and collaboration tool, for departmental data – used to be on S: drive.	Yes	Yes	Yes	Yes, with appropriate config.	Yes	User and sysadmin	Yes	Yes	Yes	Others can be given access if have federated accounts.
M365 – Teams	Collaboration tool	Yes	Yes	Yes	Yes, with appropriate config	Yes	User and sysadmin	Yes	Yes	Yes	Membership of teams may be more ephemeral and under different controls.
Home drive	User's individual data	Yes	Yes	Yes	No	Yes	User and sysadmin	No	No	N/A	Moving away to OneDrive. New staff won't have one.
Shared drive	Departmental data, repository for all Birkbeck data.	Yes	Yes	Yes	Yes	Yes, hourly snapshot	Internal as configured	No, unless user encrypts the file.	No	No direct remote access	Where you are supposed to put it if nowhere specific else.
Email	Communication tool	Yes	Use shared space and	Personal data must be encrypted.	No	Yes	User and sysadmin	Available when configured/ used.	No	Yes	Not meant for data storage

			consider recipients								
Device local storage (College-supplied computer)	Local storage	Not good practice	Drive must be encrypted and backed up	Drive must be encrypted and backed up	No	No	User and sysadmin	No, not by default	No	No, unless specifically configured	
External drive/USB sticks	Backup?	Yes	No	No	No	No	User	No, not by default	No	Needs to be physically with user or attached to device the user can remote into.	
Non-Birkbeck provided cloud solutions (e.g. Youtube, Dropbox, Google Drive)	Cloud storage	Not good practice	No	No	No	No	User and service provider possibly	No	No	Yes	Researchers needing to collaborate with external colleagues on Dropbox should ensure that the appropriate due diligence has been carried out around backup provision, licensing, identification of storage being UK/EU.

If you have any questions, please contact infosec@bbk.ac.uk for advice.