LSHTM
Data Storage Options

Public	Internal	Confidential	Highly Confidential
Information that is published for the public and/or could be disclosed with no risk.	Limited to members of the School 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.	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.	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.

LONDON SCHOOL of HYGIENE &TROPICAL MEDICINE

Storage System	Purpose	Suitability for storage/processing of data classified as per the LSHTM Data Classification & Handling Policy				Automatic back-up	Accessible to:	Data Encryption	File access auditing	Remote access	Note
		Public	Internal	Confidential	Highly confidential						
Home drive (H:)	User's own data	✓	✓	✓	✗	✓ daily	User & system admin	✗	✗	✓	Must be connected to MyFiles or Horizon to access remotely. Bulk or legacy network drive content must not be copied to SharePoint (wider guidance to follow in relation to GDPR)
Network drives (I:, J:, K:, U:)	Faculty/ Departmental data	✓	✓	✗	✗	✓ daily	Staff and RD students in designated department/faculty All staff can access U:	✗	✗	✓	
Storage on Demand	High capacity storage space for large data sets	✓	✓	✗	✗	✓ mirrored	User only unless shared	✗	✗	✓	
MyFiles	Mapped access to Home and Network drives	✓	✓	✗	✗	Provides remote access to above 3 storage solutions	User only unless shared	In-transit encryption only	✗	✓	Formally known as Filr
Isolated server in secure room	Processing of sensitive data	✗	✗	✓	✓	✗	Authorised user only	Not by default – possible to configure	✓	✗	Access is restricted on a workstation basis
Secure Server	Research data that requires long-term storage	✗	✗	✓	✓	✓ daily	Registered group members	✗	✓	✗	
SharePoint / Microsoft Teams	Collaboration tool integrated with Microsoft Office incl. Outlook	✓	✓	Appropriate permissions need to be applied	✗	✗	All staff (and ext guests) – each site has permissions applied by owner	In-transit encryption only	✗	✓	Require internet connection and are accessible from mobile devices. OneDrive is the equivalent to DropBox and supported by ITS
OneDrive	Data storage and transfer	✓	✓	Recommend encryption for personal data	✗	✗	User only unless shared	In-transit encryption only	✗	✓	
Data Compass	Sharing of reusable research outputs	✓	✗	✗	✗	✓ daily	Permissions based access	✗	Anon page views and download stats only	✓	http://datacompass.lshtm.ac.uk/
Open Data Kit	Tablet & web form based data collection & survey tools	✓	✓	✓	✓	✓ daily	Encrypted data can be accessed via web with user name and password.	✓ Fully encrypted. Decryption requires key file + user name + password	✗	✓ App & webforms work online	http://opendatakit.lshtm.ac.uk ODK is preferred over REDCAP in most circumstances due to enhanced security
REDCap	Build and manage online surveys and databases	✓	✓	✓ ODK Preferable due to enhanced security	✓ ODK Preferable due to enhanced security	✓ daily	Unencrypted data can be accessed via web with user name and password	✓ At rest and in transit. Decryption requires user name + password	✗	✓ App works online & off-grid	https://redcap.am.lshtm.ac.uk
Email	Transfer of documents from one person to another	✓	Use shared space and consider recipients	If personal data, it must be encrypted	✗	✗	Recipients only unless shared	✗	✗	✓	Not recommended for data or document storage
PC/laptop local drive	Temporary unimportant data only	Not good practice	Drive **must** be encrypted and backed up, seek Helpdesk advice		✗	Available on request: Particularly relevant for laptops (Crashplan)	Local user only (by default)	Not by default– possible to configure	✗	Not by default	Not recommended for data or document storage
External drive / USB sticks	Data storage and transfer	✓	Only when encrypted	Only when encrypted	✗	✗	User only but technically anybody if lost or stolen	✗ Not by default	✗	✓	Not recommended for data or document storage
Non-School provided cloud solutions (i.e. Dropbox)	These services are not supported by ITS. You should use caution before storing information on Google Apps, Dropbox, or any other cloud service provider. For all cloud services, including OneDrive (which we do support), you must consider the sensitivity/criticality of the information as well as research/grant restrictions and Confidentiality Agreements. As a general rule, if there are legal or reputational consequences should the information you are storing be lost, stolen, or seen by unauthorised persons or organisations, you should not use a cloud service provider to store, transmit, or process it. **Items classified as Confidential or Highly Confidential must not be stored here!** Information mgmt. and security policies are available on the School website. Guideline 1 relating to Cloud storage services applies: https://www.lshtm.ac.uk/aboutus/organisation/information-management-and-security										