Data Sharing and Storage Guidelines – Quick Reference

The guidelines help members of the University of Manitoba community to share and store university data using the appropriate tools. Please refer to the Data Security Classification for detailed definitions of Restricted, Protected, Internal and Public document types at the following link: U of Manitoba Data Security Classification

Storage Locations & Sharing Options	University Supported Systems	University-provided Departmental File Storage - On premise	University-provided Shared File Storage - Cloud	University-provided Individual File Storage	University-provided Email	University-provided Instant Messaging	Removable Storage	Personal Devices	Cloud Services not supported by the university
	e.g. Banner, EPIC, VIP, UMLearn	S: Drive	SharePoint Teams	H: Drive OneDrive	@umanitoba.ca, @myumanitoba.ca	Teams Chat, Jabber	USB, CD, DVD, External hard drive	phones, laptops, computers	e.g. Dropbox, Google Drive, Slack, Gmail
Restricted	! 1	! 1	! 1	! 2	! 3	✗ 6	! 4	! 5	✗ 7
Protected	✓	✓	✓	✓	! 3	! 3	! 4	! 5	✗ 7
Internal	✓	✓	✓	✓	✓	✓	! 4	✓	✗ 7
Public	✓	✓	✓	✓	✓	✓	✓	✓	✗ 7

For further information regarding Data Classification or Data Storage guidelines, please consult the Access and Privacy Office site for resources.

Microsoft 365 training and resource materials for Teams, OneDrive and SharePoint are available from Microsoft 365 Training and on the Microsoft 365 project site.

✓ Acceptable Usage.	! Use with Caution. Consult with IST for assistance if required.	✗ Not Recommended.
Please follow all University Policies and Procedures Always apply access permissions and manage file sharing appropriately.	1. Restrict access permissions and manage sharing links appropriately. 2. Shared drive, SharePoint, Teams and other University managed systems are preferred for collaboration and document sharing for teams and departments. 3. Minimize unnecessary copies of protected data by sharing links instead of data files. 4. Encrypt removable storage devices such as external hard drives and USB. Removable storage devices are suitable for short-term or temporary storage. Restricted, protected and internal data should only be stored on encrypted removable storage. 5. Caution is recommended when using **personal** devices to access and use university data. When using a personal device, the data should be retained and managed from a university-supported service such as email, SharePoint, OneDrive or Teams.	6. S: Drive (shared drives), SharePoint, email and Teams are preferred options for storing and sharing restricted and protected data. 7. Do not use cloud services that are not reviewed, authorized, provided and supported by the university to store or share university data as they lack the contracts or service agreements that safeguard ownership and control of university data.

Produced jointly: Access and Privacy Office, 233 Elizabeth Dafoe Library, 204.474.9462, fippa@umanitoba.ca
Information Services and Technology, 204.474.8600, servicedesk@umanitoba.ca

Issued August 2020