Research Data Sharing and Storage Guidelines – Research Not Involving Humans Quick Reference

University of Manitoba researchers who do not collect human data in their research may use this guideline as a quick reference tool to determine the appropriate platforms to share and store research data. Please refer to the Data Security Classification for detailed definitions of the data classifications. Researchers will govern their data in accordance with the Data Security Classification and any relevant terms from their research contracts or data sharing agreements. After publication, data that does not contain sensitive personal information, sensitive confidential information or intellectual property may be stored as Protected or Public Data, in accordance with the approved Data Management Plan submitted and approved by the REB.

Storage Locations & Sharing Options	University Supported Open Data Repository: E.g., Dataverse	University-provided Departmental File Storage - On premise (S or R drive)	University-provided Shared File Storage - Cloud (M365, SharePoint)	University-provided Individual File Storage (H Drive, One Drive)	University-provided Email (@umanitoba.ca, @myumanitoba.ca)	University-provided Instant Messaging (Teams Chat, Jabber)	Removable Storage	Personal Devices	Free Cloud Services not supported by the university, or contractually obligated for service
Restricted	✗	! 1	! 1	! 1	! 2,3	✗	! 4	! 5	✗ 6
Protected	! 1,2	! 1	! 1	✓	! 2,3	! 3	! 4	! 5	✗ 6
Public	✓	✓	✓	✓	✓	✓	✓	✓	✓

For further information regarding Data Classification or Data Storage guidelines and application please consult with your local IT and/or the Access and Privacy Office. Additional resources are available on the Access and Privacy Office site. Training and resource materials for Teams, OneDrive and SharePoint are available at Microsoft 365 Training and on the Microsoft 365 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 as they are secure, supported and have back-up and continuity processes in place. 3. Minimize unnecessary copies of protected data by sharing links instead of data files. 4. Removable storage devices are suitable for short-term or temporary storage and must be encrypted for restricted or protected data. 5. Caution is recommended when using **personal** devices to access and research. When using a personal device, the data should be retained and managed from a university supported service such as email, SharePoint, OneDrive, or Teams. Use a VPN where possible.	6. Do not use cloud services that are not reviewed, authorized, provided and supported, or under contract by the university to store or share research data as they lack the contracts or service agreements that safeguard ownership and control of research data. Free cloud services include platforms like Gmail and Hotmail, or a Google account.

Produced jointly by:
Access and Privacy Office, 233 Elizabeth Dafoe Library, 204.474.9462, fippa@umanitoba.ca
Information Services and Technology, 204.474.8600, servicedesk@umanitoba.ca
UM Libraries Administration, 204.474.9881, Libraries.GeneralEnquiries@umanitoba.ca
Research Ethics Board, 204.474.7122, humanethics@umanitoba.ca

Issued November 2022