Data Handling and Storage Guidelines

The University of Saskatchewan data classifications help members of the university community to identify, understand, manage, and use university data appropriately.

The data classes described below are meant to be used as recommendations in conjunction with any applicable compliance requirements, such as The Local Authority Freedom of Information and Protection of Privacy Act or Copyright Act.

Storage Locations & Sharing Options	**Institutional Systems**	**University-provided Department File Storage**	**University-provided Individual File Storage**	**University-provided Email and Instant Messaging**	**University-provided Research Storage**	**Removable Storage**	**Personal Devices**	**Non-university Cloud Services**
	Banner, RMS, UnivRS, AIM, UFriend	Jade, SharePoint, SharePoint Online, MS Teams	Cabinet, OneDrive	@usask.ca accounts, MS Teams	DATASTORE	e.g. USB, External Hard Drive, CD, DVD	e.g mobile phones, computers	e.g Dropbox, Slack, Gmail
RESTRICTED	✓	! 1, 7	! 2	✗ 7, 8	✓ 4	! 5	✗ 8, 9	✗ 10, 11
LIMITED	✓	✓ 7	✓	! 7, 3	✓	! 5	✗ 8, 9	✗ 10, 11
INTERNAL	✓	✓ 7	✓	✓ 7	✓	✓	! 9	✗ 10, 11
PUBLIC	✓	✓ 7	✓	✓ 7	✓	✓	✓	! 6, 10

All members of the university community are required to comply with all ethical, regulatory, statutory, third-party, and other contractual obligations; to use data only for the purposes for which it is collected; to observe any restrictions for its use; and to collect, store, and dispose of data in ways appropriate to risk and impact of unintended disclosure. Access alone does not authorize use of data.

! Use with Caution: Contact IT for assistance and recommendations.

1. Restrict access permissions appropriately on all university-provided departmental file storage services.
2. Jade, SharePoint, and DATASTORE are preferred options for storing restricted and limited data outside of institutional systems.
3. Minimize unnecessary copies of limited and restricted data by sharing links instead of data files.
4. Restrict access permissions appropriately on DATASTORE.
5. Encrypt removable storage devices such as external hard drives and USB. Removable storage devices are suitable only for short-term or temporary storage.
6. Do not use non-university cloud services to store or share university data as they lack the contracts or service agreements that safeguard ownership and control of university data.
7. Formal Teams created in MS Teams can be used for secure data storage, but not the general Chat/Instant Messaging portion of MS Teams.

✗ Not Recommended: Contact IT for assistance and recommendations.

8. Jade, SharePoint, and DATASTORE are preferred options for storing and sharing restricted and limited data outside of institutional systems.
9. Do not store sensitive university data on personal devices. Personal devices require increased security settings when used to access university data.
10. Do not use personal email to store and share university data.
11. Do not use non-university cloud services to store or share university data as they lack the contracts or service agreements that safeguard ownership and control of university data.