



















# Data Management and Storage Guidelines

The University of Alberta 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 UAlberta [PARIS](#), [Freedom of Information \(FOIP\)](#), and [Protection of Privacy Act](#) or [Copyright Act](#).

University Storage Options for Administrative Purposes				
Administrative Data Needs	Institutional administrative data	Administrative data that supports your team/unit	Individual use data	Person-to-person or team communication platforms
<b>**Available Solutions</b>	EDRMS, PeopleSoft, SupplyNet	<a href="#">Google Shared Drives</a> , <a href="#">Department Network Drives</a>	<a href="#">Google My Drive</a> , <a href="#">Department Network Drives</a>	U of A Gmail, Google Chat, Jabber Softphone application, Zoom
<b>Restricted</b>				
<b>Confidential</b>				
<b>Protected</b>				
<b>Unrestricted</b>				

**Personal Devices at Work Disclaimer:** It is [highly discouraged](#) to purchase and/or use removable storage devices, personal mobile devices, or non-sanctioned cloud services for work purposes. These include, but are not limited to: USB flash drives, External Hard Drives, External SSD drives, CDs, DVDs, mobile phones, computers, Dropbox, Slack, M365 OneDrive, Apple iCloud, Box, etc.

-  **Not Advised:** Refer to [Information Security policies including UAPPOL Policy](#)
-  **High Risk:** Requires [Chief Information Security Officer](#) approval via the [Privacy and Security Review Checklist](#)

\*Google MyDrive **should not be used** for any long term storage and retention practices.













University Storage Options for Research Purposes								
Research Data Needs	Active individual research	Active collaborative research	Archival	Archival	Active Sensitive Health Data	External Advanced Research Computing	Secure research storage	Sensitive Data Digital Research
**Available Solutions	*Google MyDrive	Google Shared Drive	Library Storage Archive	U of A Library Borealis-Dataverse	Data Analytics Research Core (DARC)	Access to National Digital Research Infrastructure (DRI)	Research Data Storage Service (RDSS) Coming May 2024	Sensitive Data Research Environment Coming Q2 2025
<b>Restricted</b>	!	!	!	!	✓	✗	✓	✓
<b>Confidential</b>	✓	✓	✓	✓	✓	✗	✓	✓
<b>Protected</b>	✓	✓	✓	✓	✓	!	✓	✓
<b>Unrestricted</b>	✓	✓	✓	✓	!	✓	✓	✓

**Personal Devices at Work Disclaimer:** It is highly discouraged to purchase and/or use removable storage devices, personal mobile devices, or non-sanctioned cloud services for work purposes. These include, but are not limited to: USB flash drives, External Hard Drives, External SSD drives, CDs, DVDs, mobile phones, computers, Dropbox, Slack, M365 OneDrive, Apple iCloud, Box, etc.



- ! **Not Advised:** Refer to [Information Security policies including UAPPOL Policy](#)
- ✗ **High Risk:** Requires [Chief Information Security Officer](#) approval via the [Privacy and Security Review Checklist](#)

\*Google MyDrive **should not be used** for any long term storage and retention practices.

\*\*Department/College based solutions exist outside of these solutions (eg. [HRDR](#), [Cirrus](#))

University Storage Options for Teaching Purposes			
Instructor Data Needs	Digital teaching materials used in course presentations, assignments	Collaborative work	Media files for Teaching
**Available Solutions	*Google My Drive	Google Shared Drive	<u>YuJa</u> & Canvas Studio
<b>Restricted</b>			
<b>Confidential</b>			
<b>Protected</b>			
<b>Unrestricted</b>			

**Personal Devices at Work Disclaimer:** It is highly discouraged to purchase and/or use removable storage devices, personal mobile devices, or non-sanctioned cloud services for work purposes. These include, but are not limited to: USB flash drives, External Hard Drives, External SSD drives, CDs, DVDs, mobile phones, computers, Dropbox, Slack, M365 OneDrive, Apple iCloud, Box, etc.

-  **Not Advised:** Refer to [Information Security policies including UAPPOL Policy](#)
-  **High Risk:** Requires [Chief Information Security Officer](#) approval via the [Privacy and Security Review Checklist](#)

\*Google MyDrive **should not be used** for any long term storage and retention practices.

## Institutional Data Categories

### Restricted Data

This classification is for information that is extremely sensitive and could cause extreme damage to the integrity, image or effective service delivery of the University of Alberta. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. Restricted information is available only to named individuals or specified positions. (Examples include restricted spaces, credit card numbers, social insurance numbers, and personal medical records).

### Confidential Data

This is for information that is sensitive within the University of Alberta and could cause serious loss of privacy, competitive advantage, loss of confidence in University programs, or damage to partnership, relationships and/or reputation. Confidential information includes highly sensitive personal information. Confidential information is available only to a specific function, group or role. (e.g. personnel files, including personal salary data, and 3rd party business information submitted in confidence).

### Protected Data

This is for information that is sensitive outside the University of Alberta and could impact service levels or performance, or result in low to medium levels of financial loss to individuals or enterprises, loss of privacy, loss of confidence in University programs, or damage to partnerships, relationships and/or reputation. Protected information includes personal information, financial information or details concerning the effective operation of the University of Alberta. Protected information is available to employees and authorized non-employees (contractors, sub-contractors and agents) possessing a need to know for a business-related purpose. (e.g., grades, dates of birth, and personal contact information other than University email addresses). These definitions and classifications reflect the Government of Alberta information security classification standard.

### Unrestricted Data

This is for information that is created in the normal course of business that is unlikely to cause harm. Unrestricted information includes information deemed public by legislation or through routine disclosure or active dissemination. Unrestricted information is available to the public, employees and contractors, sub-contractors and agents working for the University. Or, where the information has not been made available to the public, if it were, it would not have any harmful or negative effect. (e.g. university email addresses, accounting chart of accounts).

Excerpt from: <https://policiesonline.ualberta.ca/PoliciesProcedures/Procedures/Institutional-Data-Management-and-Governance-Procedure.pdf>

#### Links & Resources

*Institutional Data Management and Governance Procedure*

<https://policiesonline.ualberta.ca/PoliciesProcedures/Procedures/Institutional-Data-Management-and-Governance-Procedure.pdf>

*Mobile Device Encryption Policy*

<https://www.ualberta.ca/information-services-and-technology/security/encryption/index.html#:~:text=Any%20mobile%20or%20portable%20personal,infor mation%20must%20also%20be%20encrypted.>