


University of Guelph Data Storage Guidelines

The following table is intended to introduce University-approved electronic data storage solutions for various levels of data sensitivity. More detail is available in existing policies/guidelines such as the [Research Data Classification Guideline](#). This is not intended to replace existing guidelines or conflict with internal department or business unit practices. Where there is an overlap between this guideline and departmental guidelines, the more restrictive guideline should be followed.



Type of Data	Examples	Acceptable Storage Locations	Additional Considerations
Public (S1)	<ul style="list-style-type: none"> Press releases Course descriptions Convocation programs Maps, directories, etc. 	<ul style="list-style-type: none"> All storage devices and cloud solutions 	<ul style="list-style-type: none"> No restrictions on copying or storage
Internal (S2)	<ul style="list-style-type: none"> Non-public reports Internal documents Contracts (excluding research contracts) and purchase orders (PO) Operating procedures and operational guides Admission metrics 	<ul style="list-style-type: none"> Encrypted laptops, workstations, encrypted USB drives Email and Office 365 University approved 'Cloud' storage – Microsoft OneDrive and SharePoint Central File Service (CFS) Qualtrics Survey Tool 	<ul style="list-style-type: none"> Explicit owner permission required to share or exceed original purpose Encryption strongly recommended, but not required.
Confidential (S3)	<ul style="list-style-type: none"> Data protected by legislation (e.g. Freedom of Information and Protection of Privacy Act (FIPPA)) Personally identifiable information (PII) (e.g. employee ID numbers) as defined in FIPPA Student grades, class lists Research data containing PII, health information, and confidential research (by law or contract) 	<ul style="list-style-type: none"> Encrypted storage (e.g. laptop, workstation, encrypted USB drives) University approved 'Cloud' storage – Microsoft OneDrive and SharePoint Central File Service (CFS) Sanctioned University systems for student information, financial information, and human resources information Qualtrics Survey Tool 	<ul style="list-style-type: none"> Explicit owner permission required to share or exceed original purpose Encryption required for data storage (with the exception of data stored in CFS) and transmission, including via email
Restricted (S4)	<ul style="list-style-type: none"> Personal health information specifically covered by PHIPA (e.g. Student Health Services) Financial or banking information (including credit card information) Social Insurance Numbers (SIN) 	<ul style="list-style-type: none"> Encrypted storage (e.g. laptop, workstation, hardware encrypted USB) Central File Service (CFS) Sanctioned University applications for student, financial, and human resources information 	<ul style="list-style-type: none"> All considerations above for Confidential are applicable, plus: Must never be stored in any hosted or cloud environment Must not be shared via email

If you have questions or require clarification regarding the guidelines described in this document, please contact the [CCS Help Centre](#) at x 58888. Questions related to research data storage should be directed to The Office of Research.