McMaster University

Information Storage Guidelines

Introduction

McMaster community members require access to information to fulfill their roles and responsibilities within the community. Some information may be high value or sensitive, including personally identifiable information, personal health information, and intellectual property. It is the responsibility of all members of the McMaster community to exercise appropriate care and discretion when accessing digital information, and to protect the information they access, use, or store.

Failure to store information securely may lead to unauthorized access to personally identifiable information, disclosure of intellectual property, unauthorized disclosure of McMaster University information, reputational damage and monetary loss.

The guidelines in this document outline storage options available and recommended for the secure storage of high value and sensitive information and provides information storage options and alternatives to mitigate risks related to the protection of personal privacy, intellectual property and copyrighted materials, as well as safeguarding the reputation of the University. These guidelines apply to any information stored by McMaster community members on behalf of the University.

Information Storage Considerations

When deciding where to store information, consider the following questions:

- What is the value or sensitivity of the information? Does the information contain personally identifiable data, personal health information, or intellectual property?
- What is the status of the information? Is this a draft, a final document, or somewhere in between?
- Who needs to access the information? Are collaborators internal or external? Do they need to edit the information, or just view it?
- Is the information encrypted? Should it be?

The following table outlines various information types including examples, acceptable storage options and additional considerations.

INFORMATION TYPES	EXAMPLES	ACCEPTABLE STORAGE OPTIONS	ADDITONAL CONSIDERATIONS
UNRESTRICTED	**Information that is intended for use by the Public** **Teaching and Learning** - General course/program information which does not contain any information about students etc **Research** - Research data that does not contain any sensitive or personally identifiable information (if in doubt, assume that data is sensitive) - Non sensitive research documentation and forms (e.g. blank consent forms and information sheets) **Administration** - Brochures, News releases - Marketing material - Staff/faculty business contact info - Policies	**Any device or storage solution** - Local hard drive (e.g., C: drive, "My Documents") - Removable storage media (e.g., USB drives, portable hard drives, etc.) - University provided on premises file sharing and storage (e.g., UTS hosted shared network drives) - Department provided on premises file sharing and storage (e.g., department shared network drives) - University provided on premises cloud-based storage (e.g., MacDrive, MacDrop, MCloud, Dataverse) - University provided off premises cloud-based storage (e.g., Office365, including OneDrive, Teams and Sharepoint) - Department provided off premises cloud-based storage (e.g., DropBox for Business)	- No special handling required. - Official versions of course documents such as course outlines should be posted on provided University applications such as Avenue to Learn. - Research data should be stored according to protocols approved by the appropriate Research Ethics Board - Information intended for public consumption and posted to a public forum (e.g., website) must conform to University Brand Policies and Visual Identity guidelines - Use of personal off premises cloud-based storage (e.g., Google Drive, Dropbox, etc.) is discouraged

		- University applications for student, financial, and human resources information (e.g., Mosaic)	
INTERNAL	**Non-personally identifiable information for which the impact of disclosure is low.** **Teaching and Learning** - Routine correspondence **Research** - Research proposals **Administration** - Routine correspondence - Employee newsletters - Inter-office memoranda - Internal policies and procedures - Purchasing information - Purchasing requisitions	**University provided and hosted devices and storage solutions. Must be password protected.** - Local hard drive (e.g., C: drive, “My Documents”) - Removable storage media (e.g., USB drives, portable hard drives, etc.) - University provided on premises file sharing and storage (e.g., UTS hosted shared network drives) - Department provided on premises file sharing and storage (e.g., department shared network drives) - University provided on premises cloud-based storage (e.g., MacDrive, MacDrop, MCloud, Dataverse) - University provided off premises cloud-based storage (e.g., Office365, including OneDrive, Teams and Sharepoint) - Department provided off premises cloud-based storage (e.g., DropBox for Business)	**All considerations above for Unrestricted are applicable, plus:** - Reasonable precautions to prevent access by non-authorized persons. - Encryption encouraged however not required. - Use of personal cloud storage (e.g., Google Drive, Dropbox, etc.) is strictly prohibited.

		- University applications for student, financial, and human resources information (e.g., Mosaic)	
CONFIDENTIAL	**Information that is regulated or protected by legislation or contractual agreements, or intellectual property for which the impact of disclosure is high.** **Teaching and Learning** - Elements of the Student Record, (e.g., offer letters, transcripts, etc.) - Exams **Research** - Research data that may or does contain sensitive or identifiable information (e.g., human participant data) - Sensitive research-related documentation (e.g., signed consent forms) - Intellectual property (e.g., patents) **Administration**	**University hosted devices and storage solutions. Must be password protected and encrypted.** - Local hard drive (e.g., C: drive, “My Documents”). - University provided on premises file sharing and storage (e.g., UTS hosted shared network drives). - Department provided on premises file sharing and storage (e.g., department shared network drives). - University provided on premises cloud-based storage (e.g., MacDrive, MacDrop, MCloud, Dataverse). - University provided off premises cloud-based storage (e.g., Office365, including OneDrive, Teams and Sharepoint) - University applications for student, financial, and human resources information (e.g., Mosaic).	**All considerations above for Unrestricted and Internal are applicable, plus:** - Access to confidential information must be restricted to authorized individuals only. - Encryption is strongly recommended and should be used wherever technically possible. - Research data is subject to the TCPS2 which states “identifiable data obtained through research that is kept on a computer and connected to the Internet should be encrypted.” - Use of removable storage media (e.g., USB drives, portable hard drives, etc.) with encryption is discouraged, and without encryption is strictly prohibited. - Use of Department provided off premises cloud-based storage (e.g., DropBox for Business) is discouraged.

	- Personally identifiable information (PII) - Credit card information (PCI) - Financial documents - Human Resource records (e.g., faculty and staff employment record) - Tax forms and T4 slips - Passwords - Vendor Contracts		
RESTRICTED	**Highly sensitive or strategic organizational information for which the impact of disclosure is very high.** **Research** - Research data that contains restricted or highly sensitive information **Administration** - Personal Health Information (PHI) - Critically sensitive information - Strategic organizational plans and/or financial information - Sensitive meeting minutes	**University hosted devices and storage solutions. Must be password protected and encrypted. Must not be stored on removable or portable media.** - Local hard drive (e.g., C: drive, “My Documents”) - University provided on premises file sharing and storage (e.g., UTS hosted shared network drives). - Department provided on premises file sharing and storage (e.g., department shared network drives). - University applications for student, financial, and human resources information (e.g., Mosaic).	**All considerations above for Unrestricted, Internal and Confidential are applicable, plus:** - Cloud-based storage solutions, including University provided on premises cloud based storage solutions, are not appropriate locations to store restricted information. - Must never be stored in any unsanctioned storage location. - Use of removable storage media (e.g., USB drives, portable hard drives, etc.) is strictly prohibited. - Use of University provided off premises cloud-based storage (e.g., Office365, including OneDrive, Teams and Sharepoint) is strictly prohibited.

🟥			- Use of Department provided off premises cloud-based storage (e.g., DropBox for Business) is strictly prohibited.

Storage Guidelines for Recommended Use

Storage Device Security

Access to any storage device (i.e. computer, phone, etc.) must be password protected and, if working with Confidential or Restricted information, it must also be encrypted.

Removable storage devices (e.g., USB drives, portable hard drives, etc.) can be easily lost or stolen. Use of portable storage media to store University information that is not otherwise publicly available is discouraged. University sanctioned cloud storage, such as MacDrive, is recommended for collaboration and transportation/syncing between devices. If removable media must be used, please follow the guidelines above.

Avoid storing confidential information on mobile devices.

When disposing of equipment that may have been used to store any University related information, it must be cleaned appropriately: all information deleted with appropriate tools.

Collaboration

Except as authorized under the Electronic Mail (E-Mail) Protocol for Personal Information and Personal Health Information Policy (https://www.mcmaster.ca/privacy/privacy/policy/email-protocol-for-personal-info-and-personal-health-info.pdf), email is not appropriate for sharing sensitive information. Sensitive information should be stored in appropriate storage locations, and links to that information can then be shared via email. Email is not appropriate for storing documents and information.

Cloud storage is recommended for group and team collaboration as limits can be placed on access i.e., to a specific document or an entire folder, read and write permissions, encryption, and password protection or user credentials.

OneDrive is recommended when collaborating externally on non-confidential and non-restricted information, i.e., a research proposal or a marketing brochure, etc. University or department sanctioned cloud storage are acceptable alternatives.

If external collaboration is absolutely necessary for confidential information, MacDrive is recommended but encryption is mandatory. i.e., research data with another University.

MacDrive is recommended when collaborating internally on non-confidential and non-restricted information. Other University sanctioned cloud storage, i.e., MacDrop, Mcloud, Dataverse, etc., is also suitable when collaborating between departments.

MacDrive with additional encryption is recommended for confidential information. I.e., financial documents being shared between departments.

If not working on a collaboration document, consider using a network file share or MacDrive. If working with confidential or restricted information, all data and files should be encrypted.

Final Documents

Final versions of University documents such as policy, procedure, contract, etc. should be moved to a sanctioned University hosted network share if it is needed to be kept long term.

Getting Help

For assistance with any of the technologies, concepts, and actions described in this document, please contact your local IT Support staff, or the UTS Service Desk:

uts@mcmaster.ca

x2HELP (x24357)