Public Information	
Definition and Examples	Information that is classified as public can be freely disclosed without any risk to MHC or its employees. Additionally, public information does not infringe on any individual's right to privacy. Examples include, but are not limited to: • Academic Calendar, • Annual Report, • Comprehensive Institutional Plan, • Strategic Plan, • award recipients, • job postings, • marketing materials, and • organizational structure.
Storage Requirements	Original information must be stored on college authorized electronic storage environments including: • MHC network storage (Q: drive, P: drive), • MHC owned and onsite computers, • MHC authorized cloud storage environments including: • MHC licensed OneDrive (***excludes*** Google Drive) locations (mhc.ab.ca and mymhc.ca accounts). Copies of the information can be housed on non-college storage devices, or internet locations, or services.
Preferred Access and Transport Methods	**"Don't Worry About It"** • College authorized remote access (e.g. gateway service), • Internal and external email service users, • MHC licensed OneDrive and MS Teams locations, • College authorized social media, and • By linking to the appropriate page of the MHC website.
Acceptable Access and Transport Methods (if preferred method is not possible)	Can be transported on personal or college owned computing and storage devices.

Internal Information	
Definition and Examples	Information that is classified for internal use may circulate between college employees. Unauthorized disclosure or loss of this information may result in inconvenience, but is unlikely to cause financial or reputational damage to MHC, or harm to any individuals. Examples include, but are not limited to: • anonymized human subject research data, • anonymized institutional data, • internal memos, • meeting agendas (department or committee), and • meeting minutes (department or committee).
Storage Requirements	Originals and all copies must be stored on college authorized electronic storage environments including: • MHC network storage (Q: drive, P: drive), • MHC owned computers, and • MHC authorized cloud storage environments including: • MHC licensed OneDrive (***excludes*** Google Drive) locations (mhc.ab.ca and mymhc.ca accounts).
Preferred Access and Transport Methods	**"Caution - On College Owned or Authorized Computer Systems"** • College authorized remote access (e.g. gateway service) only using college owned and encrypted computing devices, • Through college authorized employee email system(s), and • MHC licensed OneDrive and MS Teams locations.
Acceptable Access and Transport Methods (if preferred method is not possible)	• Can be transported on college owned password protected and encrypted computing and storage devices, and • Through the college employee internal email service.

Confidential Information	

Definition and Examples	Access to confidential information is restricted to authorized personnel who have a specific and legitimate business need. Unauthorized disclosure or loss of this information may cause:
	• financial and/or reputational damage to MHC and its employees, and
	• harm to the individuals to which the information pertains.
	
	Examples include, but are not limited to
	• alumni information,
	• contracts with:
	  - community partners,
	  - third party service providers, and
	  - vendors,
	• diagnostic, treatment, care and health registration information,
	• donor/prospective donor information,
	• employee information including:
	  - applications,
	  - evaluations,
	  - payroll, and
	  - personnel files,
	• financial planning and management,
	• identifiable human subject research data,
	• identifiable institutional data,
	• intellectual property,
	• medical information, health status or accommodations,
	• MOUs,
	• payment card information,
	• pending litigation, formal complaints or investigations,
	• project planning and documentation,
	• prospective student/player recruitment information,
	• residence applications and resident information,
	• student information including:
	  - academic records
	  - applications
	  - attendance
	  - contact notes
	  - financial status and transactions, and
	  - system passwords.

Confidential Information	
Storage Requirements	• Original information **and all copies** must be stored on college authorized electronic storage environments that are accessible only to those employees who have a work-related need to access the material, and • Confer with Information Technology (IT) Services if such storage is not configured for you or if you have any questions.
Preferred Access and Transport Methods	**"High Caution! On College Owned or Authorized Computer Systems and Only by Authorized People"** • College authorized remote access (e.g. gateway service) on college owned or authorized devices, • Through college authorized employee email system(s) **with all college recipients** internal to the college authorized email systems. (Use caution, it is easy to accidently send emails to a wrong email address.),Confidential information accessed remotely should not be transferred to personal or public computing devices. Such information should always be housed on college authorized electronic storage environments that are password protected, and encrypted, and • Confidential information must only be accessed by employees who have role authority to access the information.
Acceptable Access and Transport Methods (if preferred method is not possible)	• If other means of access and transport are needed, consult with IT services by contacting the help desk and indicating your need to transport confidential college information, and • Confidential information must only be accessed by employees who have role authority to access the information.