Information Classification Guideline

What is Information Classification?

Information classification is the process of categorizing information based on its sensitivity and the potential harm that could result from unauthorized access, use, or disclosure. Classification helps ensure that appropriate safeguards and access controls are applied to protect individual records and information assets — such as databases, systems, applications, and documents — throughout their lifecycle. Effective information classification supports regulatory compliance, reduces risk, and improves how information is stored, shared, and managed across the University.

Purpose of this Guideline

MacEwan University is responsible for managing and protecting all information under its custody and control. Categorizing information according to appropriate sensitivity levels helps reduce the risk and impact of information breaches while supporting compliance with University policies and the secure management of information across the institution. This guideline helps staff and faculty determine the appropriate classification level to apply and understand what that classification means in practice. Correct classification supports privacy, security, compliance, and appropriate access and collaboration throughout the information lifecycle.

Classification Levels

Information classification is based on the sensitivity, potential impact, including financial, legal, or reputational consequences to the University or individual(s) in the event of unauthorized access. Proper classification ensures that information is adequately protected by role-based access.

Classification Level	Sensitivity Level	Description	Information is Intended for	Examples
Restricted	**Major** risk and harm	The information is highly sensitive, has direct legal and contractual obligations, and could cause **major risk** and harm to the University or individual(s) if breached.	Access is strictly limited to **authorized individuals**.	- Investigations reports - Confidence reports - Credit card numbers - Social Insurance Number - The Board of Governors' private meeting materials
Confidential	**High** risk and harm	The information includes sensitive elements with legal and contractual obligations, and could cause **high risk** and harm to the University or individual(s) if breached.	Access is restricted by **role-based access** for those who require the information to perform their duties.	- Personal information as defined by POPA - Contracts - Detailed infrastructure diagrams - 3rd party business information - Student assessments

Internal	**Minor** risk and harm	The information is for the University's internal operations and could cause **minor risk** and harm to the University or individual(s) if breached.	Access is intended for those who are **employed, enrolled, or are stakeholders** of the University.	- Detailed campus maps - Student and staff contact information - MacEwan student and employee ID numbers - Internal operational processes
Public	**Negligible** risk and harm	Access is available to everyone and could pose negligible risk or harm to the University or individual(s) if breached.	Everyone	- News and articles - Website content - General campus maps - Ordinary committee meeting agendas and minutes

How to Determine the Classification Level

To choose the correct classification, ask yourself three questions:

Access – Who should have access?

Consider who the information is intended for:

- **Restricted**: a specific individual, as they are directly involved, or a need-to-know requirement.
- **Confidential**: a limited group based on their role and level of access to complete their work.
- **Internal**: employees, students, stakeholders (e.g., prospective students, vendors, volunteers, contractors, visiting academics, etc.).
- **Public** – everyone or anyone.

Risk – What is the impact if this information is exposed to someone unintended?

Consider the potential impact to individuals (e.g., privacy, identity theft, reputation) and to the University (e.g., legal, financial, or reputational harm):

- **Restricted:** Major or severe impact
- **Confidential:** High impact
- **Internal:** Minor impact
- **Public:** Negligible impact

Volume – How much information is being shared?

Larger volumes of information increase risk. When in doubt, choose the higher classification. Always apply the classification based on the highest level of sensitivity, risk, or volume present.

Consider the scale of the information:

- A single record or limited data elements (e.g., first name, last name, student email)
- A large dataset involving many data elements (e.g., class list details, first name, last name, student email, personal phone number, studentID, assessment grade)

MacEwan UNIVERSITY

PRIVACY AND INFORMATION MANAGEMENT

Your Role in Protecting Information

Every individual who creates, modifies, or shares information is responsible for applying and confirming the correct classification. Taking a moment to verify classification ensures that information is accessed, shared, and stored appropriately. Consistent and accurate classification also enables effective collaboration by ensuring information is handled in line with its sensitivity.

Selecting Storage Solutions Based on Classification

Choosing the right storage platform for documents helps ensure that information is protected in accordance with its sensitivity and associated risks. Below are guidelines for storing information by classification.

Storage Platforms	OneDrive	SharePoint & Teams	Google Drive	Google Shared Drive	Local Workstation / External Storage
Information Classification Level	Restricted, Confidential, Internal, and Public	Restricted, Confidential, Internal, and Public	Confidential, Internal, and Public	Confidential, Internal, and Public	Transitory
Function	Recommended for day-to-day individual work for all MacEwan Faculty and Staff.	Recommended for storing active files and collaborating on administrative workloads and projects.	Recommended for day-to-day individual work for MacEwan Faculty.	Recommended for storing active information & collaboration for academic workloads between faculty and students.	Not recommended, as it is prone to loss and is not backed up.

Additional details on the Information Storage Solutions can be found on the MacEwan myPortal, Information and Privacy Office page.

Regular Review

Information should be reviewed when its use, access, or when the sensitivity changes. Formal periodic reviews should focus on higher-risk information, systems, and information assets. Access to the information should be reviewed when roles or responsibilities change, especially for Restricted and Confidential information. Remove access that is no longer required.

Information Retention and Disposition

The classification level of information, along with its sensitivity and risks, requires adherence to appropriate retention and disposal practices. Following the retention requirements outlined in the **University's Records Retention Schedule** helps to minimize the risks associated with retaining sensitive information longer than necessary. Restricted and Confidential information contains highly sensitive or personally identifiable information that can have serious consequences in the event of unauthorized access, information breach, and improper destruction. Please refer to the **University's Records Destruction Procedure** to ensure that information is securely and appropriately disposed of.