RECORDS CLASSIFICATION AND HANDLING POLICY

RECORDS CLASSIFICATION AND HANDLING POLICY			
Effective Date	June 30, 2016	**Cross- Reference**	1. Protection of Privacy Policy 2. Records Management Policy
Responsibility	Vice-President Administration	**Appendices**	
Approver	Executive Council		
Review Schedule	Every 5 years		

1. Policy Statement

1.1. Grande Prairie Regional College ("GPRC" or the "Institution") processes and stores sensitive and personal information as part of its business operations. Such data must be appropriately protected to prevent unauthorized disclosure.

2. Background

2.1. Protecting sensitive information assets is necessary to prevent unauthorized disclosure of confidential data or a privacy breach, as well as to prevent violation of contractual engagements and privacy regulations which could result in litigation.

2.2. Protecting sensitive data requires a clear identification of such data. Appropriate measures and practices should be tailored to the various forms such data can take and for the various operations that can be applied to this data (i.e. data processing, transport and storage).

3. Policy Objectives

3.1. The objective of this policy is to establish formal requirements for classifying and handling Institution information assets, to prevent unauthorized disclosure.

4. Scope

4.1. This policy applies to:

4.1.1. All types of information created, processed, stored or exchanged, whatever the format – i.e. paper as well as electronic records, emails, databases, etc.

4.1.2. All Institution offices, campuses and learning centres.

4.1.3. All students, employees, consultants, contractors, agents and authorized users accessing Institution IT systems and applications.

5. Definitions

5.1. "Information" is the knowledge, facts or communication created or obtained under any format or media. It includes linked data such as a message, document, experimental data, picture, book, or a whole data bank. Information could be an official or transitory record, or a resource material including library publications or knowledge.

5.2. "Record" is information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

5.3. "Personal information" is information related to an individual that can be used to identify, contact, or locate a single person, or to identify an individual in context. This includes an individual's name, home address and phone number, age, sex, marital or family status, an identifying number, religion, ethnic background, health status, financial information (such as banking or credit card information), educational history, and so forth.

5.4. "Data Owner" is an individual with the authority to make decisions on information, including approving the creation, classification and access to a specific data set.

5.5. "Data Steward" is a person responsible for the management of information, including handling, processing or storage controls of a specific data set.

5.6. "Users" includes students, employees, consultants, contractors, agents and authorized individuals with access to GPRC IT systems and applications.

6. Guiding Principles

6.1. All information (irrespective of its format) created, received, stored, and processed by the Institution must be classified according to the sensitivity of the information content and the risks of an unauthorized disclosure.

6.2. The level of classification must be indicated on all sensitive documents.

6.3. A change in classification may occur only after formal approval from the data owner, IT Director or Information and Privacy Coordinator.

6.4. The management of classified information must follow the requirements defined in the Protection of Privacy Policy and the Records Management Policy. Specifically, all users and data stewards must follow the requirements in this Policy, the Protection of Privacy Policy and the Records Management Policy.

6.5. Handling requirements, in line with the level of classification, must be applied during the entire life of such information, from the creation of the data until its destruction.

6.6. Stakeholders must clearly identify all information assets and the owners of specific information assets. Owners are responsible for ensuring that appropriate safeguards are applied to their information. Owners can authorize the possession of the information to custodians to provide proper protection and care in an ongoing, operational environment.

6.7. GPRC information must be classified into one of the following categories:

Classification	Definition	Handling requirements
Confidential	Information whose unauthorized disclosure, compromise, or destruction could result in major impact such as severe reputation damage; significant damage to GPRC employees, contractors or contractual partners; or serious financial impact to the Institution or its employees. Such confidential information may include, but is not limited to the following: • Personal information such as social insurance numbers, professional license numbers, names of spouse, children, parents, guardians, beneficiaries, marital status, physical description, education, financial matters, medical or employment history and other non-public personal information pertaining to individual faculty, employees, students, alumni, donors, etc.; • Personnel records, employee performance, payroll records, and other personnel information; • Faculty appointment, promotion, termination and data records; • Student educational and financial records; • Unpublished research results, including manuscripts and correspondence; • Data concerning research subjects; • Donor and alumni information; • Medical information; • Budgetary, business, financial, departmental, internal reports, memoranda, correspondence, contracts, strategic or planning reports and information, surveys, internal audit reports, etc that contain personal information.; • Privileged Information about or provided by third parties (i.e., information covered by non-disclosure agreements, contracts, business plans, non-public financial data, computer programs, etc.); • System passwords and security codes; and • Litigation or other formal charges or complaints records and documents pending or in the process of investigation.	Confidential information must be: ▪ Labelled as “confidential”. ▪ Stored in a locked cabinet or storage area when processed in a physical form (such as print-outs or removable media, USB key, external hard drive or disk), and be transmitted using a tracking service. ▪ Stored and transmitted using encryption software and accessed through a login and password, when processed in an electronic format (such as computer, mobile device, email, server or the Internet).

Classification	Definition	Handling requirements
Restricted	Information that is neither Public nor Confidential. This information includes information that the Institution and its employees have a legal, regulatory, or professional obligation to protect and is typically limited to employees and contractors of the Institution. For example: • Financial information; • Business plans; • Contracts; • Draft press releases not yet approved for release; • Sensitive project documentation; • Internal policies; and • IT system configuration.	Restricted access information must: ▪ Not be released to, or be directly accessible by, the public. ▪ Be shared only with authorized users, on the internal network, through professional email, or authorized file transfer systems. ▪ Be transferred with caution over the Internet, only to Institution users or authorized partners. ▪ Be stored in a physically secured location, where possible, when in a physical form (such as print-outs or removable media, USB key, external hard drive or disk). ▪ Be stored in "access-restricted" file shares or folders using the network domain login and password, or controlled by the owner of the device.
Public	Information that can be disclosed to anyone without violating legal or regulatory requirements, including an individual's right to privacy. Knowledge of this information does not expose the Institution to financial loss, embarrassment, or jeopardize the security of its assets. There will be no impact on the Institution, its staff, and students if this type of information was mishandled or accidently disclosed. For example: • Staff brochures • Web content • Job postings • Advertisements • Pamphlets	Public information must be handled as per the Communication Policy.

7. Roles and Responsibilities

Stakeholder	Responsibilities
Executive Council	• Approve and formally support this policy.
Vice-President Administration	• Review and formally support this policy.
Information and Privacy Coordinator	• Develop and maintain this policy. • Take proactive steps to reinforce compliance of all stakeholders. • Review and approve any exceptions request relative to the requirements in this policy.

Stakeholder	Responsibilities
Institution Management, Supervisors or Representatives	• Explain the terms of this policy to employees and students and assist users to understand the requirements of this policy. • Ensure that all users follow the requirements of this policy.
Contract Administrators and Managers	• Follow the guidelines provided in this policy when performing due diligence and assessment of the risks related to security for any new contract. • Ensure that responsibilities and obligations of each party to the contractual relationship are outlined in the contract executed between the Institution and the contractor/sub-contractor.
Human Resources	• Present each new employee or contractor with the existing GPRC policies, upon the first day of commencing work with GPRC. • Support all employees and students in the understanding of the policy requirements.
All users (Employees and contractors, Students, Visitors and Volunteers)	• Comply with the applicable requirements of this policy at all times. • Report all instances of non-compliance with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible.

8. Exceptions to the Policy

8.1. Exceptions to the guiding principles in this policy must be documented and formally approved by the Vice-President Administration.

8.2. Policy exceptions must describe:

8.2.1. The nature of the exception.

8.2.2. A reasonable explanation for why the policy exception is required.

8.2.3. Any risk created by the policy exception.

8.2.4. Evidence of approval by the IT Director.

9. Inquiries

9.1. Inquiries regarding this policy can be directed to the Information and Privacy Coordinator.

10. Amendments (Revision History)

10.1. Amendments to this policy will be published from time to time and circulated to the Institution community.