TITLE: INFORMATION ACCESS AND PROTECTION OF PRIVACY POLICY

POLICY STATEMENT:

Red Deer College (RDC) is committed to the security, privacy, and confidentiality of the personal information of its Board Members, employees, students, alumni, donors, clients, contractors (community members). RDC is governed by provincial legislation enacted by the province of Alberta through the *Freedom of Information and Protection of Privacy (FOIP) Act*. RDC manages the collection, use, distribution, and retention of personal information in accordance with FOIP and other applicable legislation, regulations, and procedures.

PURPOSE:

The policy describes how RDC governs the collection, use, disclosure, and retention of personal information by members of the RDC community in alignment with information security, records management and other RDC related policies.

SCOPE:

This policy applies to:

- RDC employees, students, volunteers, Board Members, alumni, donors, contractors, clients, and agents providing services on behalf of RDC.
- All personal information in the custody or under the control of RDC in whatever form or medium.

PRINCIPLES:

1. Policies at RDC:
    - 1.1 Treat all persons fairly and respectfully.
    - 1.2 Are non-discriminatory and non-intrusive.
    - 1.3 Incorporate open, honest and timely communication.
    - 1.4 Are made in a timely manner.
    - 1.5 Provide appropriate confidentiality and privacy.
    - 1.6 Provide appropriate access to the College and education.
    - 1.7 Ensure that all persons have access to informed support regarding policies, procedures, rights and responsibilities.
    - 1.8 Operate with clear written expectations for conduct and handling of complaints.
    - 1.9 Meet all regulatory standards.
    - 1.10 Maintain and clearly state a high standard of instruction and administration in all areas of educational programs and services.
    - 1.11 Are communicated in alternate forms to those who require such accommodation.

2. The following principles apply specifically to this policy:

   2.1 RDC is responsible for the personal information in its custody or under its control in accordance with the FOIP Act.

   2.2 All decision and/or actions involving personal information collection, use, disclosure, retention, and disposition are conducted in consultation with the FOIP Coordinator at privacy@rdc.ab.ca.

DEFINITIONS:

Access: An Individual's right to access their personal information in the custody, or under the control of RDC. The availability of records in the custody, or under the control, of RDC for a person to view or copy.

Accuracy: personal information collected, use or disclosed are correct, up-to-date and valid.

Authentication: a process that identifies an individual before access to information is granted.

Collection: an action or process of gathering, acquiring, recording, or obtaining personal information from any source, by any means, and in any format for the purpose of conducting RDC business.

Confidentiality: refers to restrictions on the accessibility and dissemination of information.

Consent: voluntary agreement to collect, use, and/or, disclose personal information in a manner consistent with the FOIP Act.

Control: the authority to managed records under RDC's custody, including restricting, regulating and administering use, disclosure or disposition.

Custody: records that are in the physical possession of RDC.

Disclosure: disclosing personal information in a manner consistent with the FOIP Act.

Employee: includes, in relations to a public body, a persona who performs a service for RDC as an appointee, volunteer or student or under a contract or agency relationship with RDC.

Freedom of Information and Protection of Privacy (FOIP) Act: a statute of Alberta, Chapter F-25

FOIP Coordinator: is the individual who is assigned by the President to be responsible for managing access and privacy responsibilities both internally and externally.

Formal Access Request: a request for information which cannot be answered through the existing procedures or that is not routinely disclosed or not actively disseminated.

Indirect Collection: when information is collected from another source(s) other than the individual the information is about.

Informal Access request: Information that can be obtained without applicant having to submit formal request.

Integrity: refers to the reliability and authenticity of information assets. Specifically, the integrity of records refers to their trustworthiness as evidence, their ability to stand for the facts they are about, and their trustworthiness over time**.**

Personal Information: any recorded information that can identify a person such as name, home or business address, social insurance number (SIN), gender, family status, student records (for example grades, ID), and age. This list is not exhaustive, refer to section 1(n) of the FOIP Act.

Privacy Breach: the loss of, unauthorized access to, or disclosure of, personal information.

Privacy Impact Assessment: A process that assist RDC departments in reviewing the impact that a new initiative, software or application upgrade may have on an individual privacy.

Records and Information: all information, documents, and data, regardless of media or format, which demonstrates a business transaction or decision by the College.

Retention: retention of personal and confidential information in accordance with the RDC Records and Information Management policy that meets legal, regulatory and business requirements.

Third Party: a person, group of persons, or an organization other than an applicant or public body.

Violation: any violation of this policy may be subject to disciplinary action in accordance with RDC policies, collective agreements, and provincial and federal laws. Employees must report all privacy breaches that he/she is aware of or has become aware of. Failure to report is a direct violation of this Privacy Policy.

GUIDELINES:

1. **Accountability**:

   1.1 The RDC President is responsible for ensuring RDC is compliant with the FOIP Act.

   1.2 The RDC President may delegate the responsibility for managing personal information accuracy, access, collection, use, disclosure, and retention.

   1.3 The delegate, normally the FOIP Coordinator, is responsible for application of the policy across RDC except where specified in the delegation table.

   1.4 All employees must make every reasonable effort to become acquainted with the requirements of the FOIP Act, RDC policies, associated procedures and practices.

   1.5 Employees are responsible for all personal and confidential information under their custody or control and must treat all personal information they receive access to in accordance with the FOIP Act and RDC policies, associated procedures and practices.

   1.6 Employees must report any privacy breach to their supervisor and the FOIP Coordinator. Employees must follow the Privacy Breach Response and Reporting Procedures in the event of a suspected privacy breach.

1.7 The FOIP Coordinator will provide relevant training and support to employees of RDC on matters related to the FOIP Act.

1.8 The following college officers have been assigned control of records as indicated. The FOIP Coordinator shares these responsibilities and can act on their behalf if they are not available.

- Alumni records - Director, Community Relations
- Employment records - Vice President, Human Resources
- Financial records - Vice President, College Services and CFO
- General Records – Data and Information Specialist
- Institutional Research - Executive Director, Strategic Planning and Analysis
- Library Records – Director, Library Information Common
- Medical records – Manager, Health, Safety and Wellness
- Student records – Registrar

2. Accuracy:

2.1 RDC makes reasonable efforts to ensure that personal information used to make decisions that directly affect an individual is as accurate, complete and up-to-date as necessary for the purpose for which it was collected.

2.2 RDC corrects or updates personal information where the individual believes that an error or omission has been made during collection upon notification by the individual. To request a correction of personal information, individuals are able to contact the officer responsible (Refer to section 1.8)

2.3 If an office holding information is unable to make a correction for any reason, an individual may file a request for correction in writing to the FOIP Coordinator. If there is a satisfactory grounds for personal information to be corrected, then correction will be made as soon as possible.

2.4 RDC makes every effort to send corrected personal information to any third party the information was shared with during the year prior to when the correction made.

3. Access:

3.1 Individuals have the right to access records or personal information that belongs to them in the custody or under the control of RDC in accordance with the FOIP Act. RDC also considers specific and limited exceptions specified in the FOIP Act.

3.2 Not all records held under the custody or control of RDC would require a formal request procedure, some records can be accessed through informal request, where the record is routinely disclosed or actively disseminated.

3.3 In the event where a request to access information cannot be routinely disclosed, the individual may file an access to information request with the officer responsible which is forwarded to the FOIP Coordinator. All formal requests must be in writing, detailed enough to enable RDC to locate the requested record, and accompanied with the applicable fees. (except where the applicant is unable due to circumstances that makes it impracticable).

3.4 Access to personal information is provided in accordance with the RDC Access to Information (FOIP Request) Procedure and the Access to Student Academic Records policy.

3.5 RDC must make every effort to assist an applicant requesting to access information under its custody and control.

3.6 A request by an RDC employee for access to the personal information of a student or another employee should be directed to the officer responsible. (Refer to section 1.8). Access will only be granted if the requested information is based on a business need to know.

4. Collection of Personal Information:

RDC does not collect personal information for commercial marketing or for distribution to any private organization, unless specifically authorized by an individual at the point of information collection.

4.1 RDC only collects personal information for the following purpose:

4.1.1 the information relates directly to and is necessary for an operating program or activity of RDC or

4.1.2 the collection of personal information is expressly authorized by an enactment of Alberta or Canada; or

4.1.3 the information is collected for the purpose of Law enforcement.

4.2 RDC will collect personal information directly from the individuals the information is about, except where there is a reasonable requirement to collect from another source(s), and where indirect collection is permitted under FOIP Act.

4.3 Consent of an individual is obtained before information is collected, except as required by law, law enforcement, or in emergency situations. In those limited circumstances personal information may be collected without consent of the individual.

4.4 A FOIP notification statement stating the purpose of collection, specific legal authority for collection and the contact of who can answer questions must be on all college forms (paper or electronic) used to collect personal information.

5. Use and Disclosure of Personal Information:

5.1 RDC does not use or disclose personal information other than for the stated purpose(s) at the time of collection, except where required by law or through consent of the individual the personal information is about.

5.2 RDC may disclose to a third party or make public personal information under the following circumstances:

5.2.1 The disclosure is required and authorized with respect to the FOIP Act; or

5.2.2 The disclosure does not conflict with the unreasonable invasion of privacy provision of the FOIP Act; or

5.2.3 Personal information contained in the student record may be disclosed to: RDC academic and administrative units for planning and research activities, federal and provincial agencies for reporting requirements, contracted or public health care providers including collaborative educational agencies, funding agencies, and workplace agencies as required, and the Students' Association of RDC through data sharing agreements.

5.2.4 Personal information contained in the employee record may be disclosed to: law enforcement, associations including FARDC, AUPE, CUPE, and for tax purposes.

5.2.5 It is not considered to be an unreasonable invasion of employee's privacy to disclose the following information: employment status, RDC address, telephone, email address, job title, rank or job family, salary range, discretionary benefits, or personal information already in the public domain.

5.2.6 Personal information contained in the alumni record may be disclosed for the purpose of RDC fund-raising activities, where consent has been collected.

6. Personal Information Assurance/Security:

RDC protects personal and confidential information by making every reasonable security arrangement against the risk of unauthorized access, collection, use, disclosure, or destruction.

6.1 RDC protects personal information under its control and in its custody from unauthorized access, collection, use, copying, modification, disclosure, disposal, or intentional destruction by enforcing security control measures. (Refer to Appendix A)

6.2 Personal and confidential information under the custody and control of RDC is protected according to the sensitivity of the information. (Refer to Appendix B)

6.3 RDC monitors its information management program to ensure confidentiality, integrity, availability, and authenticity of personal information is preserved.

6.4 RDC conducts privacy impact assessments on initiatives that collect, use or disclose personal information to ensure that personal information risk is identified, mitigated or brought under control such that the impact is minimal.

6.5 RDC takes reasonable steps to prevent unauthorized collection, use, disclosure, or disposition of personal or confidential information by providing employees with FOIP training and limiting access to information systems.

7. Retention:

7.1 RDC retains personal information for as long as necessary or relevant for the identified purpose of collection or as required by law.

7.2 RDC retains personal information used to make a decision about an individual for a reasonable period of time to allow the individual opportunity to obtain access to it.

7.3 RDC maintains systematic control and schedules for records retention and destruction which applies to personal information under its custody and control. Personal information that is no longer relevant to the identified purpose is destroyed or deleted in accordance to records management policy.

PROCEDURE:

Refer to the following procedures in the event of an access to information request or a privacy breach:

- Access to Information (FOIP Request)
- Privacy Breach Response and Reporting Procedures.

OFFICER RESPONSIBLE: Vice President College Services

POLICY CATEGORY: Non-Academic

RECOMMENDING AUTHORITY: Service Council

CONSULTATION FOR REVIEW: Deans' Council, Service Council, Risk Manager, Data and Information Management Specialist, Head of Security, Chief Information Officer, Registrar, Human Resources.

POLICY REVIEW DATE: July 2019

EFFECTIVE DATE: July 1, 2017

REVISION HISTORY: January 1, 2005 (Freedom of Information and Protection of Privacy)
July 1, 2017 (revised and renamed Information Access and Protection of Privacy)

RELATED POLICIES:

- Access to Student Academic Records
- Web Site Privacy
- Communication and Information Systems Acceptable Use
- Information and Technology Security
- Information and Technology Management
- Records and Information Management
- Risk Management
- Security Policy (under development)
- Student Rights and Responsibilities
- RDC CCTV and Use of CCTV (under development)
- Authentication and Password Control (standard)
- Physical and Environmental Security (standard)

CONNECTION TO BOARD POLICIES:
All RDC policies support relevant Board of Governors policies.

Appendix "A"

Security Controls:

Personal and confidential information under the control and custody of RDC is protected in accordance to the FOIP Act, the protection of privacy is requirement by the Act and the following are controls used to ensure that personal and confidential information are protected.

1. Administrative Controls

1.1 RDC develops and periodically reviews policies, procedures, and guidelines as deemed necessary.

1.2 The need for security and privacy of information under the custody or control of RDC is addressed as a requirement of employment for all staff.

1.3 All employees with access to personal and confidential information should make effort to familiarize themselves with the Privacy Policy and Privacy Breach Response and Reporting Procedures.

1.4 A Privacy impact assessment may be required whenever a new software or system is to be deployed or there is an upgrade to an existing system or software used to collect personal information. It is important to contact the Risk Manager prior to implementation.

2. Technical Controls

2.1 Security standards, procedures, and guidelines are developed to meet business, legal and regulatory needs.

2.2 The requirement that all personal devices used to complete College business meet all College information technology standards, as well as College information management standards. Employee should contact the IT Service Desk to receive instructions on how VDI can be accessed using their personal devices.

2.3 Employees using network and mobile device sign-on that include passwords, are required to change passwords at predetermined intervals.

2.4 Passwords are to be kept confidential at all times and should not be written down, kept in the open, or shared.

2.5 Creation of passwords should follow the RDC Authentication and Password Control standard. Passwords can only be changed by the user or authorized personnel from the RDC IT department.

2.6 If a user suspects their password is no longer secret, it must be changed immediately.

2.7 An employee's account should have the least privilege necessary for the employee to do their job.

2.8 An employee's access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a position or role change, or termination of employment with or by the College or the employee.

2.9 Account details will only be divulged to the employee or student requiring any account action after a proof of identity has been established.

2.10 All employees or students must be assigned with a unique identifier for any College system.

2.11 The account must not be used in any manner that may reveal or compromise the account details.

2.12 Personal and confidential information must be encrypted when sent over external or public networks and must be stored only on systems owned or contractually controlled by RDC for college business.

2.13 Do not fax personal information unless that is the only available means of communication. Use fax cover sheet whenever personal or confidential is to be faxed.

3. Physical Controls

3.1 Standards and procedures are developed and reviewed periodically to meet the changing physical needs.

3.2 All records containing personal or confidential information held onsite or offsite must be kept in a safe and secure manner. Paper records should be kept in a locked cabinet.

3.3 Personal or confidential information should not be left unattended or displayed publicly.

3.4 Use additional physical barriers, where appropriate, to prevent unauthorized access or physical contamination to sensitive, personal, and confidential information area.

3.5 Rooms that hold personal and/or confidential information records must be locked or protected at all times.

3.6 Rooms that hold personal and/or confidential information records should have appropriate protection against fire, water or other reasonably anticipated environmental threats.

3.7 Rooms used to store computer equipment that are not in use are kept locked at all times.

3.8 Use of appropriate intrusion detection systems, such as motion and perimeter alarms, audio and video surveillance.

3.9 Shredding bins should be kept in areas not physically accessible by the public.

Appendix "B"

Information Classification

RDC makes every reasonable security arrangement to protect personal and confidential information against unauthorized access, collection, use, disclosure, or destruction. One of the ways to maximize the effort of protecting information is creating an information classification that shows the information type, risk impacts and a recommended security protection.

Classification	Definition	Examples of Records includes but not limited to	Sensitivity level
Level 1: Unrestricted Public	• Information deemed to be routinely disclosed or actively disseminated. • Information created in course of daily RDC transaction unlikely to cause any harm to RDC or its community. • Information deemed to be public by legislation. • Information that exist in the public domain.	Business contact, Job advertisement, roles and responsibilities, salary range, discretionary benefits, program enrollment, names of registered students, public event attendee, award receipt, telephone directory, announcements, and annual reports,	Not Sensitive. No direct Impact.
Level 2 Internal use Protected	• Information held within the College not approved for public disclosure. • Information disclosure may likely cause harm, financial loss or RDC reputation damage. • Information loss or disclosure can impact service level and performance.	Grade, date of birth, CCIDs, employee and student IDs, personal contact information, departmental internal memo, and minutes	Moderately sensitive. Business disruption. Password
Level 3 Confidential	• Information that is very sensitive. • Can cause serious harm to RDC like financial loss, reputation damage, competitive edge, loss of confidence. • Information breach that may require notification of affected individual and Office of Information and Privacy Commissioner.	Student enrollment status, personnel file, law enforcement related information, 3rd party business information submitted in confidence, employee discipline file, identifier database, driver's licence or passport, and admission application,	Highly Sensitive.

Level 4 Restricted	• Information loss or disclosure can cause severe or extreme damage to RDC integrity and reputation. • Information disclosure that lead to severe harm to individuals and/or RDC. • Information disclosure that impact service level, and performances.	Credit card numbers, social insurance numbers, health care numbers, budget draft, medical history, and records.	Extremely sensitive.

Examples of the Privacy Policy Application that affects the entire RDC Community Members	
Situation	**RDC Privacy Policy Applies**
Administrative/General	
An employee or student wonders what privacy legislation RDC is subject to.	Yes
A faculty, school, department, or employee decides to download a new application or software that will collect, use, disclose, or dispose of personal or confidential information.	Yes
A faculty, school, department, or employee intends to employ a cloud base services that collects, uses, discloses, stores, or disposes of personal or confidential information.	Yes
A faculty member receives a formal access request	Yes
An employee collects, uses, discloses, or disposes of personal or confidential information not compliant with the FOIP Act or Regulation.	Yes
The process involved in making a formal access request pertaining to personal or confidential information.	Yes
An RDC community member makes an inquiry on the protection of personal and confidential information.	Yes
A staff member is concerned with the privacy implication of conducting RDC business on networks other than RDC's network or storing personal or confidential information on storage devices other than RDC storage servers.	Yes
A staff member overheard a possible privacy breach from a colleague and is wondering if he or she can make a report even if the breach is not directly related to him/her.	Yes
How long can personal information be retained for?	Yes
How can I determine what constitutes personal information privacy with information supplied through survey?	Yes
Do I need a FOIP statement on every form (Electronic and paper) that is used to obtain personal information?	Yes
Human Resources	
A staff member or a hiring staff member makes note about a potential applicant during a job interview, he/she is wondering what to do with the note after the interview.	Yes
An Instructor makes a request to have access to his/her evaluations by students.	Yes
An Instructor makes a request to have access to his/her reviews by peers.	Yes
An instructor has concerns with the disclosure of his/her middle name on timetable, blackboard, or other related educational material.	Yes
A student or employee requests a change to his/her personal information.	Yes

What are the satisfactory ground to enable a change to my personal information for example;
• Legal name change
  • Can I provide court affidavit?
  • A written note from my lawyer?
  • Another government ID that shows the change?
• Marital status change
  • Can I provide a marriage certificate?
  • Another government ID that shows the change?
• Gender change
  • Can I provide a legal document from the court?
  • A written note from the hospital to proof gender change?
• Title Change
• Address Change
  • Is a new proof of address enough?
• SIN
  • Can I provide my last T4 tax papers that show the new SIN?
  • Can I provide a document from Service Canada?
  • Is my new SIN document enough as a proof?
	Yes

Faculty	
A faculty member discloses student's personal information that may result in a breach of privacy.	Yes
A faculty or staff member discloses student grades in a hallway or an open area.	Yes
A faculty member returns a student's marked papers, reports, or essay through another student that the personal information is not about.	Yes
A student refuses that his/her photograph, audio, or video is disclosed in any manner by a faculty member.	Yes
A faculty member prints a student's picture using a public printer (e.g. Walmart photo printer)	Yes
A faculty member receives a call from a student requesting access to his/her own personal information.	Yes
A faculty member receives access inquiry from a third party requesting to know a student's records that may include timetable, attendance, progress, grades, fee payments, etc.	Yes
A faculty member uses personal information collected for other purpose not stated at the time of collection.	Yes
A faculty member discusses with another staff member over the phone or a public area about a student's personal information.	Yes
A faculty member discloses a student personal information to a potential employer.	Yes
Student	
A student has concerns with his/her personal information being released to a collection agency.	Yes

A student requests to know why his/her personal information is released to the law or local enforcement.	Yes
A student wants to know why his/her personal information was not disclosed to a spouse or close relative.	Yes
A former student requires to know why his/her personal information related to honor or award received, attendance or participation in a public event, or graduation related information was disclosed.	Yes
Student makes a request to access an evaluation form completed by an employer who may have accepted him/her on placement.	Yes
A student's marks or attendance is disclosed to a funding agency.	Yes
A student request for correction of his/her personal information under the custody or control of RDC.	Yes