Manual

Information Access and Privacy Manual	
Policy: Information Access and Privacy Policy	
Category: Administrative	**Approval Date:** October 29, 2020
Procedure Owner: Vice President, College Services	**Effective Date:** October 29, 2020
Procedure Administrator: Manager, Risk Services & Procurement	**Review Period:** 5 Years
Associated Documents Learning Management System Policy	

Table of Contents

PURPOSE

As a public body, Red Deer College (RDC) is governed by the provisions set forth by the *Freedom of Information and Protection of Privacy Act* (FOIP). This manual expands upon the Access & Privacy Policy and outlines the information RDC faculty and staff may need to know to perform their job duties at RDC.

SECTION 1: FOIP Overview

FOIP was created to foster openness and accountability in Alberta's public bodies. It strives to create a balance between the public's right to know and the individual's right to privacy. FOIP has two main parts.

The first is the freedom of information, the provisions in which anyone can apply for and receive access to public body records. This is often called a FOIP request or Access to Information request. It allows anyone the "right" to access any record created in the context of RDC business. Although the public has a "right" to request access, it does not mean that access to the record, in part or whole, is granted.

The second part of the act is concerned with the protection of personal information. These provisions govern RDC employees in their day-to-day job duties and includes the collection, use, disclosure, accuracy, retention, and security of personal information that is within our custody or control. All faculty and staff of RDC, as public body employees, are responsible for complying with the second part of FOIP. Willful contravention can result in individual fines up to $10,000.

What is Personal Information

Personal information under FOIP is any information that can make someone personally identifiable, including:

- name, address, phone number, email,
- race, origin, religious or political beliefs,
- age, sex, gender, family status,
- identifying numbers (ex. student ID, SIN, Driver's License),
- photographs or video, biometric information (ex. fingerprints, facial patterns), blood type, genetic information,
- health or mental health information including physical or mental disability,
- education, financial, employment, or criminal history,
- opinions from an individual, or opinions about an individual.

Services Offered

At RDC, FOIP resides under Risk Services. The FOIP Coordinator duties fall to the Access & Privacy Coordinator, with the Manager of Risk Services acting as a proxy.
The Access & Privacy Coordinator can help you or your department with:

- Answering questions related to the Access & Privacy, including the legislation
- Addressing breaches of personal information in a prompt manner
- Completing Privacy Impact Assessments on new software
- Developing and providing FOIP training for your department
- Developing procedures to protect personal information from unauthorized access, collection, use, disclosure, loss, or destruction

SECTION 2: FOIP Training

FOIP training is available to all RDC employees. This training aims to teach employees how to collect, use, disclose, correct, store, maintain, and destroy personal information in compliance with the FOIP act. The training is delivered through Blackboard and it is encouraged that all employees take the training. Service Alberta also provide basic FOIP training that can be accessed on the Service Alberta website. Risk Services will also provide department specific FOIP training upon request. FOIP training is valuable for all employees as all employees are responsible for complying with the provisions set forth with the legislation.

SECTION 3: Notification Statements

Anytime there is a collection of personal information we must inform the individual of the purpose for the collection of the information, what legal authority allows us to collect that information, and contact information for someone that is knowledgeable about the collection of information. This notification statement should be delivered in the appropriate mode for the communication. For example, written at the top or bottom of a form, given verbally when collecting personal information over the phone, or on a sign at the counter of a reception area.

Each item of information we collect must be necessary and have a strong justification for why it is needed for the operation of the program or activity in question. We cannot collect extra personal information "just in case." Below is a sample FOIP statement, simply replace the red italicized text to correspond to the situation.

This personal information is being collected for the purpose of insert your reason for collection, and in compliance with the provisions of the Freedom of Information and Protection of Privacy Act of Alberta, section 33(c). If you have any questions about the collection of this information, please contact insert business title here, Red Deer College, 100 College Blvd., Box 5005, Red Deer, Alberta T4N 5H5, Telephone: 403 insert contact number here.

SECTION 4: Best Practices

Collection

Collect personal information directly from the individual unless there is an exception under FOIP to collect the information indirectly.

Collect only the minimal amount of personal information necessary to operate the program or activity. Do not collect extra personal information "just in case" (ex. Health care numbers).

Use

Use personal information in alignment with the purpose for which the personal information was collected (described in the FOIP notification statement at time of collection) or a consistent purpose, or with the consent of the individual.

Disclosure

Control the disclosure of personal information and only disclose to other RDC employees if that personal information is necessary for them to perform their job duties. Only provide the minimum amount of personal information necessary. The disclosure should align with the purpose that the information was originally collected or a consistent purpose. If you are unsure whether the disclosure is permissible under FOIP, please do not hesitate to contact privacy@rdc.ab.ca.

If an external person or entity is requesting personal information about another individual, ensure the individual, whom the information is about, consented to the disclosure that information to the person or entity that is requesting it. If consent cannot be obtained, contact privacy@rdc.ab.ca.

Publicly Available Personal Information

Certain personal information can be disclosed under FOIP as it is not considered an unreasonable invasion of personal privacy. Routinely disclosed business contact information, limited to name, business title, work phone number, work email address, fax number, and work address can be publicly disclosed.

Information about an RDC employee's classification, salary range, discretionary benefits, or responsibilities are also an allowable disclosure under FOIP.

You may be able to disclose some former student information if it would not be an unreasonable invasion of an individual's personal privacy. Under FOIP, you can disclose if a student was enrolled in a program, graduated from RDC, if they received an award/honor (such as an RDC degree, diploma, or certificate), or if they were in attendance or participated in a public event or activity related to RDC. If the former or graduated student has asked that this information not be disclosed, then it would not be an allowable disclosure under FOIP.

Access & Security

Only record professional observations not personal opinions, so create records with access in mind.

Be cognizant when recording sensitive information in documents, such as meeting minutes, as then can become subject to a FOIP access request.

Develop security questions to verify individual's identity prior to disclosing their personal information verbally to them.

Train staff about understanding the importance of protecting personal information and have staff acknowledge their obligation to protect personal information.

Develop procedures for your department that involve handling personal information with privacy in mind.

Be aware that the more sensitive the personal information is, the higher the risk for significant harm and must make reasonable safeguards to protect personal information, so the greater the sensitivity of the personal information the greater the safeguards need to be.

Protect personal information by employing physical safeguards (locked cabinets and doors), technical safeguards (screen protectors, setting a lock-out time on computer, password protecting external drives, such as USBs), and administrative safeguards (clean desk policy, verifying individuals and their right to access information, limit amount of information left on voicemails).

Retention & Disposal

If a decision is made about an individual, this personal information must be kept for a minimum of one year, so that the individual has a reasonable opportunity to obtain access to it, or longer as identified in RDC's Records Taxonomy Retention Schedule.

Only keep personal information only as long as is needed, then securely destroy the information by ensuring no copies exist electronically (in "sent" or "deleted" folders or computer's recycling bin) or physically (by placing them fully in a locked confidential recycling bin). Contact IT Services, if you are disposing of hard drives or other data storage devices, IT services has a secure destruction bin for these types of items.

Recording/Photographing Events

Recording of public events may occur from time to time, it is recommended that notice should be given to those attending the event that recording or photographs may be taken and what these will be used for, such as promotional material. This allows individuals the option to request that their image not to be disclosed. This is especially important if the group is small enough and the individuals are easily identifiable, and in a situation such as this, it would be best to obtain consent from the individual by having them sign the RDC Consent to Use Personal Image form.

SECTION 5: Faculty

Access to Reference Letters

Students may gain access to closed letters of reference of which they are the subject of since the letter contains personal opinions about them. Letters of reference, written as part of admission to a graduate program, may be disclosed to the student because it affects their career opportunities and the faculty member always has a right to refuse writing the reference letter. This disclosure does not apply to letters conferring a benefit, such as a scholarship or award.

Access to Exams

A student has a right to request access to their own exams, which can be considered a part of the student's educational history and personal information. However, if information like questions, instructions, or reading passages are going to be used again on future exams, RDC has a right to redact or sever these before releasing the answers to the student.

Access to Student Placement Evaluations

A student can request access or for a copy of their evaluation form that was completed by an employer, who accepted the student on placement. This evaluation can be considered part of the student's educational history and personal information. However, if the evaluation contains personal information about other individuals, this information would be severed prior to access or release.

Access to Teaching Materials and Research Information

Certain materials are excluded from access under FOIP, these include teaching materials produced within post-secondary educational bodies, research information produced by faculty, and questions that are to be used for examinations or tests.

Collecting or Returning Student Assignments & Exams

Course work and exams contain personal information and should not be viewable or available publicly and should be collected and returned in a manner that prevents easy viewing by other individuals.

Posting Grades Lists

Grade lists should only be posted and displayed using RDC's Learning Management System, as per the Learning Management System Policy.

Providing Employment References for Students

You must have student consent prior to disclosing information about a student's performance, grades, or suitability for the job to a potential employer.

Retention of Student Assignments & Exams

Instructors must retain student marks earned from assignments, exams, and projects that were used to assign a final grade to a student for a period of one year, and in compliance with RDC's Records Taxonomy Retention Schedule

You are not required to keep copies of graded work if they are returned to the student. If the instructor is retaining the record, they should secure them in a locked area or on a password protected device.

Recording Online Learning Sessions

When students or individuals partake or interact during the recording of learning activities (including lectures), and other educational services, there is a potential for the collection of personal information (such as name, images, opinions, etc.). Below are best practices when planning to record:

- A FOIP notification should be provided in writing or verbally. Here is a handout that can be provided to students that will assist in notifying them about the recording of online learning sessions.
- Individuals should be informed prior to recording on how the recording will be used and shared, and who it will be shared with.
- Individuals who do not want to participate in the recording should be able to remove themselves from participating verbally or visually without repercussions or compromising their ability to engage in learning.

Recordings/Photographs in the Classroom

Classrooms are not considered public spaces because the institution controls who has access to the classroom. Consent from the individual is needed prior to recording/photographing them.

Student Recording in the Classroom

There may be times that a student needs to record in the classroom. For example, when they require accommodations by the College based on their individual needs. Although, FOIP does not apply to students individually collecting, using, and disclosing information, students should obtain permission from the faculty member prior to the recording, as the recording may be

considered academic material belonging to the faculty member. Depending on the nature of the recording, other student in the classroom may need to be informed prior to recording as well.

Using Student Course Work

It may be helpful to use student course work from time to time. If student course work is used it is considered disclosure of personal information under FOIP and could also involve matters of copyright and, therefore, it requires consent from the student. There is a Consent for Use of Online Student Coursework form available on RDC's website.

SECTION 6: Privacy Breaches

Red Deer College (RDC) aims to protect personal information under its custody and control against unauthorized access, collection, use, disclosure, or destruction. Any incident of unauthorized access, collection, use, disclosure, or destruction is investigated by Risk Services to ensure privacy, security, and the protection of personal information at RDC. This section outlines the steps taken in response to an incident where there has been a breach of personal information through unauthorized access, collection, use, disclosure, or destruction.

Definition

According to the Office of the Information and Privacy Commissioner of Alberta, a privacy breach occurs when there is unauthorized access, collection, use, disclosure, or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the *Freedom of Information and Protection of Privacy Act* (FOIP Act) or the *Health Information Act* (HIA). Unauthorized access to personal information includes:

a) Access by the public, where there is no right to access;
b) Access by a public body's employees, if those employees do not need to see the personal information in the course of their duties;
c) Situations in which information is stored in an unsecured manner such that someone can obtain unauthorized access.

Breach Causes and Recommendations

Breach Type	Recommendations
Human Error	• Double-check addresses/emails/fax numbers before sending • Always bcc for mass emails • Ensure correct fax number prior to fax and then confirm fax was received • Always ask identity verification questions or ask for proof of identification prior to disclosing personal information to unknown individuals • Passwords should be kept confidential at all times and not written down or shared
Theft/Loss	• Personal information must be protected when taking work home (encrypted USB, not leaving computer or records in an unattended environment) • Paper records should be in a secured locked area or cabinet

	• Ensure computer has a lock screen timer set or ensure you do not leave your office unlocked or unattended
Cyber Attack	• Emails should be permanently deleted on a routine basis if considered temporary records. Any email that is a record, or documents a business decision, it should be saved as a pdf and stored in a folder with appropriate access controls • Change your passwords regularly • Create complex, long, unique passwords that you do not reuse on other sites • Avoid clicking on attachments or links from unknown sources or email addresses, if you do click on anything suspicious contact IT services immediately • For further tips, IT Services has some wonderful Knowledge Base Articles found here
Inadequate Access Controls	• Segregate files on electronic systems to only those who need access for their job duties • Audit access to shared folders regularly to ensure appropriate access is in place

Employee or Department Breach Procedure

1. Contain and Report
   a) Any employee or department that becomes aware of an unauthorized access, use, disclosure, or destruction of personal information should take immediate action to contain the breach. If the breach was a Cyber Attack, contact IT Services to help contain the breach.

   b) Report the breach to Risk Services as soon as possible by phone at 403-356-4987 or email at privacy@rdc.ab.ca. Provide general details regarding the breach such as:
      - The circumstances of the breach (ex. who was involved, when and how did it occur)
      - How it was discovered and who discovered it
      - The possible cause/s of the breach
      - What personal information was breached
      - What administrative, physical, or electronic safeguards were in place (ex. locked doors/cabinets, alarms, password protection, encryption, policy or procedures)

Risk Services Procedure

2. Investigate and Assess Risk
   Upon receiving notification of an incident, Risk Services will conduct a breach investigation following the Privacy Breach Process Flowchart, and will conclude all investigations by completing a Privacy Breach Report. Depending on the details of the incident, additional follow up may occur with those involved in the discovery or containment of the breach,

any individuals whose information was involved in the breach (if needed to assess severity), or any respective departments that the breach may have affected.

3. Notification
   Based on the results of the investigation, the Access & Privacy Coordinator may consult with the Risk Services Manager and/or the Vice President of College Services in the decision to notify the affected individuals and/or the Office of the Information and Privacy Commissioner.

4. Recommendations
   If further breaches of the same type can be avoided through implementation of new processes or procedures, Risk Services may suggest recommendations to improve the security and protection of personal information. The Access & Privacy Coordinator may also work with departments, or the institution, to inform and educate on the responsibility to protect privacy and to prevent further loss, unauthorized access, or disclosure of information. The department head, if not already informed of the breach, will receive notification regarding the breach with general details of the incident and any actions that occurred as a result of the breach.

SECTION 7: Privacy Impact Assessment

Privacy Impact Assessments (PIA) analyze and identify the potential privacy risks with software systems that collect, use, or disclose personal information. A PIA takes place prior to using a new software or changing an existing software system. This assessment provides RDC the opportunity to develop or utilize appropriate mitigation strategies to minimize risk to personal information. Unlike the *Health Information Act* of Alberta, the FOIP act does not have a mandatory Privacy Impact Assessment requirement but does state that we "must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction." Red Deer College acknowledges this provision and values the privacy and integrity of its personal information.

By recommending a PIA be completed for all new systems we are demonstrating to the Office of the Information and Privacy Commissioner (OIPC) that the privacy risk associated with our systems have been assessed, and treated appropriately with the privacy and security of personal information in mind. This assessment looks at the physical, technical, and administrative controls of the software, vendor, and/or department and analyzes the security against the sensitivity of the personal information being collected or stored in the system. Recommendations for further controls can be made to further reduce risks to personal information.

If the personal information being stored in the system is considered highly sensitive, and a breach of this type of information, would cause significant harm to an individual, then a formal PIA is completed and submitted to the Office of the Information and Privacy Commissioner (OIPC) for review and acceptance. This is done to ensure that we have thoroughly analyzed all potential risks involved with using the software. Acceptance of a PIA from the OIPC is not considered an approval to use the software, it is simply acceptance that RDC has considered and addressed

relevant privacy considerations and that reasonable efforts to protect personal information has been made.

Contact privacy@rdc.ab.ca if you or your department are looking to use new software or are making changes to an existing software to start the privacy assessment process.

SECTION 8: Access to Information Requests

Any person has a right to access any record in the custody or under the control of RDC, including records containing personal information about the applicant. These are called Access to Information requests or FOIP requests. There are two types of requests: informal and formal.

Informal Access Request

Informal access requests, generally, are made by an individual attempting to gain access to their own personal information. These requests can be submitted directly to the department that holds their personal information. If the department cannot informally release the personal information, the individual would be informed to submit a formal request to gain access.

Formal Access Request

Formal access to information requests are processed through Risk Services. Below are the steps for a formal access to information request:

1. Application
   Request to Access Information Form should be filled out and submitted by:
   a) Email - privacy@rdc.ab.ca or
   b) Mail - FOIP Coordinator, Red Deer College, 100 College Blvd, Box 505, Red Deer, Alberta, T4N 5H5

2. Fees
   Personal Information - There is no initial fee for requests for an individual's own personal information or the personal information of an individual for which they are entitled to represent, unless there are photocopying fees which exceed $10.

   General Information - For requests of information, that is not personal information, the initial fee is $25.00 and additional fees, as per the FOIP Regulation, may be required to fulfill the request. If the total cost of processing the request is more than $150, the applicant will be asked to pay a 50% deposit.

   Payment for any applicable fees can be paid:
   In-person – At the Fees Office at Red Deer College's main campus during the hours of 8:30am to 4:30pm, Monday to Friday.
   Mail – To Cashier's Office, Red Deer College, 100 College Boulevard, Box 5005, Red Deer, Alberta, T4N 5H5
   Phone – Call Cashier's Office at 403.342.3132

3. Redaction

The individual or department, which holds the record, will be contacted and the records will be retrieved. Once record copies are retrieved, personal and/or sensitive information may need to be redacted or severed according to the provisions within FOIP. These provisions will be listed on the record beside the redacted information for reference.

4. Release
   The final record copies are prepared for disclosure. Any outstanding balance of the fees is collected, prior to release of the records. Every effort is made to complete all requests within 30 calendar days, as specified by FOIP. Though extensions may be applied for larger access to information requests.

SECTION 9: Personal Information Corrections

Any individual who believes their personal information within the custody or control of RDC contains an error or omission can request a correction of that personal information by contacting the department or individual that holds their information.

SECTION 10: Accessing Records

Student Records

Student Access

Students can access their academic record through:

- TheLoop - to view personal information, grades, schedules and fees.
- The Registrar to view personal information contained in their electronic and paper records.

Appropriate identification must be provided to RDC prior to viewing the electronic or paper record or to make changes to the academic record. A copy can be provided upon request but the contents of the record are property of RDC. Students can make a request to the Registrar to correct their information or to apply, or remove, a Confidential Hold to their Academic Record.

Staff Access

The Registrar restricts and controls access to student academic records. Staff access to student academic records is on an as-needed basis for the purpose of conducting business. Only those portions of the academic record relevant to the business need will be accessed.

Electronic record access requests are directed to the Student Information System Coordinator who will designate access and determine training required based on the staff member's role. Access is determined on the basis of a need to know in order to conduct business.

Paper record access requests are directed to the Administrative Assistant, Registrar's Office, who will retrieve the record and arrange for viewing in private. The paper record must remain in the custody and control of the Registrar's Office.

Access to electronic or paper records can be revoked by the Registrar should there be a compelling reason to do so.

Human Resource Records

Access requests to an employee's personnel file is considered an informal access request and employee's should be able to access the personal information in their file. If this process fails, a formal written request can be made, see Access to Information requests above. AUPE and CUPE collective bargaining agreements have articles/provisions that discuss access to Employee's personnel file, please refer to your collective bargaining agreement for more information.

Shredding Bin Access

Generally we view any materials dropped into the College's shredding bin consoles as destroyed, but there may be critical times that access is deemed necessary. Access to these bins/consoles for the purpose of search or retrieval will be granted on a case-by-case basis. If access is granted, only authorized retrievers will be able to access the shredding console and only the intended document requested for retrieval will be retrieved from the bin/console. The authorized retrievers are: the Access & Privacy Coordinator, the Manager of Risk Services, the Manager of Security and Emergency Response; and the Materials Management Coordinator. Please contact privacy@rdc.ab.ca or one of the above individuals to begin the process of retrieval.