Policy Name	**ACCESS TO INFORMATION AND PRIVACY**		
Policy #	**722**	Category	HUMAN RESOURCES
Steward	Manager, Human Resources	Date Approved	Aug. 13, 2025
Next Review Date		Date Reviewed or Revised	

POLICY

Suncrest College is committed to the appropriate use, handling, retention and disposal of the personal information of current and past learners, employees, Board Members, and members of the public.

PURPOSE

The policy explains the College's privacy and security practices as it relates to all personal information in the possession of the College, and may be supplemented by specific policies, procedures, and legislation.

PRINCIPLES

1. **THE COLLEGE**

- Suncrest College is a "Local Authority" pursuant to The Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP). As such, the college is responsible to protect the personal information it acquires in the course of business operations, provide appropriate access to records in its possession, and ensure that staff and third parties working with the College comply with this policy, LAFOIP, and any other relevant privacy legislation that may apply to the collection, use and disclosure of personal information of any kind.

2. **CONSENT**

- Suncrest College will collect personal information with consent, though in some cases that consent may be reasonably implied.
- Personal information shall not be used or disclosed except for the specific purpose for which it is collected. Subject to the Act, individuals are entitled to access their own

personal information and to request correction of the personal information where the individual believes there is an error or omission.

- The College and its employees will take reasonable and prudent measures to protect personal information from unauthorized collection, access, use, disclosure, or destruction.
- personal information will be accessed by authorized employees only for the specific purpose for which it is collected.
- personal information will be stored in a manner which limits access to authorized employees only. This will include:
    i. Storing personal information in locations which are not generally accessible to all employees and/or the general public.
    ii. Securing the rooms and/or filing cabinets containing personal Information during those times that an authorized employee is not present.
    iii. Restricting access to personal Information that is stored in an electronic format to authorized employees by requiring the entry of usernames and passwords.
    iv. Employees working from remote locations will ensure that their laptops or other mobile devices are not left logged in and unattended.

3. USE OF PERSONAL INFORMATION

The College may only use personal Information:

- For the purpose(s) for which it was obtained or compiled, or for a use consistent with that purpose.
- For a purpose permitted, authorized, or required by the Act; or
- For any other purpose provided that the explicit consent for such use has been provided by the individual to whom the personal Information relates, or by someone duly authorized to provide such consent on behalf of that individual.

4. DISCLOSURE OF PERSONAL INFORMATION

The College will only disclose personal Information to Third Parties or allow it to be made public:

- For the purpose(s) for which it was obtained or compiled, or for a use consistent with that purpose.
- For a purpose permitted, authorized, or required by the Act.
- For a purpose which is expressly authorized or required by an enactment of the Government of Canada or the Province of Saskatchewan; or for any other purpose provided that the explicit consent for the disclosure has been provided by the individual to whom the personal Information relates, or by someone duly authorized to provide such consent on behalf of that individual.

5. ACCESS AND CORRECTION OF PERSONAL INFORMATION

- The College will make reasonable efforts to ensure that all personal Information in its possession or under its control is as complete and accurate as is required for the purpose(s) for which it was collected.
- Subject to any exemptions or restrictions set out in the Act, or in any other enactment of the Government of Canada or the Province of Saskatchewan, individuals shall have the right to access personal Information about themselves which is in the possession or under the control of the College.
- In the event that any of the personal Information in the possession or under the control of the College is incorrect, incomplete or otherwise inaccurate, the individual to whom that personal Information relates has the right to request College will review and confirm the corrections and provided that it is satisfied that a correction is warranted, the College will make the correction as soon as reasonably possible.

6. ACCESS GUIDELINES

- The personal information of prospective, current and past learners and employees will be protected and access limited, where within the control of the College, to Suncrest College staff requiring the information as part of provision of normal services, to a limited set of third parties who work with the college to provide services and programs, and to those who make proper access requests and are entitled to the information per the Act.
- Subject to the Act, individuals are entitled to access their own personal information upon a written request and to request correction of the personal information where the individual believes there is an error or omission.
- Upon written request, learners may request that copies of their learner record be forwarded to themselves or to an identified third party. Where the record kept by Suncrest College is not the learner's official record (i.e.: transcript information housed at brokering institutions), learners will be advised to contact the brokering institution for an official record.
- Third party access request may be granted in appropriate cases. The affected learner or employee will be advised if his/her information has been requested and cannot be "de-identified" to comply with the request to give him/her an opportunity to object.
- Access to information may be declined or granted on a restricted basis if Suncrest College determines that any provision contained within the Act is applicable.

7. DISCLOSURE

Suncrest College may release information where a case of authorized, justified or legally required release is established. These may include:

- Release of personal information in response to a Court Order or formal legal or public investigation.
- Release information to appropriate emergency contacts in the event of an emergency or a safety or security threat to any individual.

- Release of select information to government departments for the purposes of statistical analysis and research, ensuring that the information's confidentiality is protected to the fullest extent possible.
- Release in other situations that are specifically permitted by LAFOIP.
- Release to a limited number of third-party partners who provide services related to the delivery of Suncrest College programs and services; or
- Release in order to collect a debt owing to Suncrest College.

8. RETENTION

Suncrest College retains personal information for as long as needed to fulfill the purposes for which it was collected, and for as long as needed to comply with Operational Policy 806 Records Retention.

9. INTERNAL PRIVACY

Many employees are responsible for sensitive and personal information, which is handled in the course of daily business. Some considerations include:

- Employees should not confirm the presence of a learner in a college program or his / her whereabouts to outside parties except in the case of a police investigation or emergency as directed by an out-of-scope employee.
- When preparing student or employee information for valid release, the copied documents should be marked "Copy."
- Employees must ensure that personal information is not left unsecured when the employee is away from their work area. This would include making sure the work areas are locked and / or any files or reports are properly secured if the work area cannot be secured.
- All employees need to consider the nature of printed information to evaluate whether it contains personal or sensitive information and needs to be shred.
- Shredding should be done in a timely fashion, so sensitive information is not lying around unsecured for extended periods of time.
- Employees using college credit cards must control their use and distribution of the credit card number and be aware of the possibility of fraud.
- Employees should take due care and attention when emailing or faxing sensitive and confidential information. It is recommended to set up confirmation of receipt and consider whether it is necessary to send any personal information in order to carry out the necessary task. Limit the distribution to only those recipients who have legitimate "need to know."
- Employees must ensure their laptops, USB's or other mobile devices are password protected and not left logged in and unattended .
- If an employee's mobile device or USB or laptop is lost or missing, this must be reported immediately.

SCOPE

This policy applies to all personal information and knowledge obtained by the College regarding applicants, current/past students, current/past employees, members of the Board of Directors and members of the public who share information with the College or its employees a part of the delivery of College programs and services.

DEFINITIONS

Personal Information: Personal information in the context of the College will include information about an identifiable individual that is recorded in any form as defined in Part IV, Section 23 of LAFOIP, and typically includes but is not limited to the following:

a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual.
b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved.
c) information that relates to health care that has been received by the individual or to the health history of the individual.
d) any identifying number, symbol or other particular assigned to the individual.
e) the home or business address, home or business telephone number, fingerprints or blood type of the individual.
f) the personal opinions or views of the individual except where they are about another individual.
g) correspondence sent to a local authority by the individual that is implicitly or explicitly of a private or confidential nature and replies to the correspondence that would reveal the content of the original correspondence, except where the correspondence contains the views or opinions of the individual with respect to another individual.
h) the views or opinions of another individual with respect to the individual.
i) information that was obtained on a tax return or gathered for the purpose of collecting a tax.
j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or
k) the name of the individual where:
    i. it appears with other personal information that relates to the individual; or
    ii. the disclosure of the name itself would reveal personal information about the individual.

PROCEDURES

REPORTING A BREACH

Step 1: Reporting the Breach

1. Any employee who becomes aware of a possible breach of privacy involving personal information in the custody or control of the College will immediately document and inform his or her immediate supervisor.
2. The supervisor will inform the responsible out-of-scope supervisor and will verify the circumstances of the possible breach.
3. As soon as the breach has been confirmed to have or have not occurred, the supervisor will inform the College Privacy Officer.
4. This confirmation will occur within 24 hours of the initial report.

Step 2: Containing the Breach

The College Privacy Officer will take the following steps to limit the scope and effect of the breach. These steps will include:

1. Work with appropriate College staff to immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, or correcting weaknesses in security, and
2. In consultation with College officials, notify the police if the breach involves, or may involve, any criminal activity.

Step 3: Evaluating the Risks Associated with the Breach

To determine what other steps are immediately necessary, the College Privacy Officer, working with other College staff as necessary, will assess the risks associated with the breach.

Step 4: Notification

Notification can be an important mitigation strategy in the right circumstances. The key consideration overall will be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed.

Step 5: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, the College Privacy Officer will investigate the cause of the breach and identify actions to safeguard re occurrence.

The ***Manager, Human Resources,*** is the designated Privacy Officer at Suncrest College.

The primary purpose of the Privacy Officer is to serve as a resource within the College on issues related to access to information and privacy, including compliance with ***The Local Authority Freedom of Information and Protection of Privacy Act***

Questions about this privacy statement, access to information, or concerns about your privacy may be directed to our Suncrest College Privacy Officer:

Manager, Human Resources
200 Prystai Way
Yorkton, SK S3N 4G4
t.mykytyshyn@suncrestcollege.ca

Additional Resources

Office of the Saskatchewan Information and Privacy Commissioner
503-1801 Hamilton St
Regina, SK S4P 4B4
1-877-748-2298 Toll Free or 1-306-787-8350
E: webmaster@oipc.sk.ca
Website: www.oipc.sk.ca

LEGISLATIVE AND COLLECTIVE AGREEMENT REFERENCES

The Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP)

The Local Authority Freedom of Information and Protection of Privacy Regulations

LINKS TO OTHER RELATED POLICIES, DOCUMENTS, AND WEBSITES

N/A