

PART 1: GENERAL INFORMATION

Initiative Title:	Copilot Chat
Department:	College-wide
Initiative Lead (PIA Drafter) Name and email Address:	Sybil Harrison (Associate Vice-President, Education & Innovation) Evan Hilchey (Associate Vice-President, Administration) Ted Pennell (Chief Information Officer) Farzaan Nusserwanji (Associate Director, IT Security)
Privacy Officer Assigned:	Ann Behennah

Initiative overview

Copilot Chat is now available as part of the standard offering of Microsoft 365, licensed for use to all Camosun employees and students (A3 Educational license). Copilot Chat is the only generative AI tool licensed by the college and it meets established privacy and data security standards. The college's AI Taskforce identified Copilot Chat as the recommended AI tool for use in teaching, learning and college operations. In Summer 2025 the availability of the Copilot Chat will be promoted to all employees and students. At that time documented guidelines will be provided to employees and students and will include guidance on how to use the tool in compliance with the institutional policies.

Copilot Chat can be accessed through a user's 365 account, through a Camosun authenticated Teams application or by web-based Outlook.

PIA scope

All Camosun employees and students have access to Copilot Chat through the college's Microsoft 365 application. This PIA addresses use of Copilot Chat at the college and accountability to the college's Protection of Privacy Policy and Standards of Conduct Policy.

The use of add-on licenses for individuals (additional cost) for access to Microsoft 365 Copilot for use in applications (Word, Excel etc.) is out of scope, and will be covered by a separate PIA. Other Generative AI (ChatGPT, Gemini, Grammarly etc.), and AI tools embedded in other software or applications (e.g. Google translate, Microsoft Word editor and spell check) are also out of scope.

The obligation of employees and students to comply with other college policies such as Copyright, Academic Integrity, Student Misconduct etc. are out of scope.

1. Is this an administrative/operational, teaching and learning, or a research initiative? Select all that apply.

- | | |
|--|---|
| ☒ Administrative/Operational | ☐ Research (Contact Research Ethics Board at rebchair@camosun.ca) if you have not already) |
| ☒ Teaching and Learning | |

2. Has a PIA previously been completed for this initiative?

- ☐ Yes ☒ No ☐ Not sure

3. What activities will occur within the initiative?

Copilot Chat is a generative AI tool available to all employers and students through the college's Microsoft Level 3 License. Copilot Chat is a prompt-based tool and is used to generate content, create images, analyze data, write code, provide editing feedback on writing and communications, summarize documents and other tasks suitable for generative chat AI tools.

Copilot Chat may involve incidental sharing of personal information. Section 32(a) of the BC Freedom of Information and Privacy Act allows for use of personal information under the custody or control of the college, in alignment with the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.

Use of Copilot Chat where incidental sharing of personal information may occur include:

- summarizing meeting minutes and related materials
- generating communications such as emails, letters, CamNews announcements etc.
- generating or refining website content
- conducting general research, brainstorming and idea generation
- generating or checking code, calculations etc.
- analyzing anonymized data

Copilot Chat may be used by employees and students for purposes not involving sharing personal information. Examples include:

- generating teaching materials (lecture materials, assignment questions etc.); although this activity may have Copyright policy implications
- writing and editing support; although this activity may have Copyright or Academic Integrity Policy compliance issues implications

Some uses of Copilot are not acceptable. Examples include

- reviewing resumes, cover letters and other application materials
- making decisions about employee performance and related decisions

- grading assignments and papers with identifying student data (name, C#, personal anecdotes etc.)
- evaluating student applications
- analyzing non-anonymized data
- submitting confidential 3rd party business information (e.g., evaluating an RFP)
- Analyzing confidential financial information

4. Types of data or information potentially collected, used, stored, disclosed, or accessed

- Names (first and last) of employees, students, business partners, community members
- Comments attributed to individuals
- Information about college systems and processes
- Email addresses
- Work and home addresses
- Photographs of individuals
- Student records
- Employee records

5. Did you list Personal Information in question 6? [Personal Information](#) is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

- ☐ Yes ☒ No (a general reference is made)

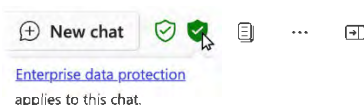
6. Mitigation of unintentionally collected personal information?

Copilot Chat uses enterprise data protection. Encryption and strict security measures protect information from unauthorized access.

- Encryption Data is encrypted in transit (TLS 1.2+) and at rest (BitLocker AES-256)
- Access control and authentication: Limited to Microsoft 365 permissions; multifactor authentication is mandatory for employees, and voluntary for students

Under the current Microsoft license, employee and student prompts and responses are not shared back to large-language models (LLM). Users can delete prompts and responses.

Users must login with their Camosun credentials which are protected with multi-factor authentication. The highly visible green shield alerts users that Enterprise data protection applies to the chat.



All information generated by Copilot Chat will remain in Camosun's Microsoft 365 environment. Data centres are primarily in Canada (Azure Cloud), but some data may be processed outside of the country.

Users of Copilot Chat will be provided explicit guidance on its use and will be asked to avoid inputting personal information (as listed in Q.4) or sharing sensitive or confidential information. Users will be advised to replace personal information in prompts with initials or aliases. The college's Acceptable Technology Use Policy O-1.1 will be updated in Fall 2025 and will outline circumstances where use of Copilot Chat is prohibited and will state that only licensed tools should be used in the conduct of college business, including teaching.

7. Does the initiative involve integration between Camosun College IT systems and Third-Party systems?

☐ Yes

☒ No

☐ N/A

Parts 2 to 12 not applicable

Part 2: COLLECTION

FIPPA sets out rules for public bodies and their employees to collect of Personal Information. Unauthorized collection is prohibited. This section will help you identify the legal authority for **collecting** Personal Information and confirm that all Personal Information elements collected are necessary for the purpose of the initiative.

8. Whose Personal Information is collected in this initiative? Check all that apply.

- | | |
|---|---|
| ☐ Students | ☐ Former employees |
| ☐ Prospective students | ☐ Service provider employees |
| ☐ Former students | ☐ Donors or other constituents |
| ☐ Alumni | ☐ Volunteers |
| ☐ Employees | ☐ Other community members |
| ☒ Other _____ | |

9. How frequently will the initiative collect Personal Information?

- ☐ Single instance of collection within one semester or quarter
- ☐ Ongoing collection up to a single year
- ☐ Ongoing collection over more than one year
- ☐ Other _____

10. How many individuals' Personal Information will be collected?

- ☐ 1 - 50 ☐ 51 – 500 ☐ Over 500

11. If the initiative involves a Third Party, are you able to test the product to see what personal information it collects?

- ☐ Yes ☐ No ☐ N/A (No Third-Party product involved)

12. For what purpose will the Personal Information be used? (check all that apply)

- ☐ It is necessary and directly related to college operations.
- ☐ It is necessary and related to requirements stated in college bylaws, policy, and procedure.
- ☐ It is collected because collection is required or authorized under local, provincial, or federal law. Be prepared to directly cite the section of a particular law that applies if asked.

- ☐ It is collected for determining suitability for an honour or award including a scholarship, prize, or bursary.
- ☐ It is being collected for a quality assurance or improvement initiative that has been approved by the college Executive.

How will you reduce the risk of collecting unnecessary Personal Information? (Check all that apply.)

- ☐ The initiative will only collect specific information deemed necessary for and directly related to the initiative
- ☐ The initiative will use forms with primarily closed-ended questions and minimal open-ended questions
- ☐ The initiative will use forms with drop-down menus
- ☐ The initiative will have documented data gathering and aggregation processes for open ended submissions or fields
- ☐ The Department needs Privacy Officer review and support because none of the above apply

- 13.** FIPPA Collection Notice: When collecting Personal Information, FIPPA requires that you provide a collection notice (except in limited circumstances). Please fill in the template collection notice below and remove bold and square brackets.

*Camosun College ("Camosun") collects your Personal Information in accordance with section 26 of the Freedom of Information and Protection of Privacy Act ("FIPPA"), R.S.B.C. 1996, c.165 for the purposes of **[explain purposes]**. If you have any questions about the processing of your Personal Information, please contact privacy@camosun.ca.*

Please ask the Privacy Office for assistance drafting your collection notice if your initiative requires indirect collection of Personal Information (i.e. if a service provider collects Personal Information from students or employees on behalf of Camosun College). The Privacy Office may recommend changes to the FIPPA Collection Notice that you draft above.

PART 3: USE

FIPPA sets out requirements and restrictions related to use of Personal Information. This section will help you identify the legal authority for **using** Personal Information and ensure that the use of Personal Information is limited to the original purpose for collection.

- 14.** What is the intended use of the Personal Information collected? (check all that apply)
- ☐ The Personal Information will be used for the purposes checked off in Question 14
 - ☐ The Personal Information will be used for secondary purposes, and I have a consent notice attached as an appendix to this PIA that meets the requirements found in FIPPA regulations. I will work with the Privacy Office to determine if secondary use is appropriate and compliant with FIPPA.
 - ☐ The Personal Information will be used for a purpose for which the information may be disclosed to the public body under section 33. The Privacy Office will attach the relevant section number to this selection if it applies.
- 18.** How will you ensure that parties using the Personal Information will use it only for the purposes stated in 17 above? Check all that apply.
- ☐ Documented department information management practices and training
 - ☐ Documented use restrictions communicated from your department to another Camosun College department
 - ☐ Written contract between Camosun College and a Third Party including explicit conditions
 - ☐ The Department needs Privacy Officer review and support because none of the above apply
- 19.** Does your initiative use Personal Information to make decisions that directly affect an individual?
- ☐ Yes ☐ No
- 20.** What is the intended impact of the decisions that are being made that directly affect an individual? (check all that apply).
- ☐ Directly affects academic status or grades
 - ☐ Directly affects how an individual accesses their courses, campus activities, or student supports
 - ☐ Directly affects employment status, employee remuneration, or contract opportunities, and pay
 - ☐ Directly affects how employees and service providers will complete their work
 - ☐ Directly affects how employees access campus activities and support services
 - ☐ Directly affects the College's capacity to protect individuals from harm
 - ☐ Directly affects the College's capacity to interact with and support external parties
 - ☐ N/A – The decisions are not intended to have a direct impact on individuals

21. Who will be using the Personal Information collected by this initiative? (Check all that apply and provide details.)

Your department:	[put N/A if a service provider manages all Personal Information]
Other Departments at Camosun College:	External Partners and Service Providers:
[put N/A if no other departments at Camosun College manage the Personal Information in this initiative]	[Put N/A if there are not any External Third Parties including Service Providers managing the Personal Information in this initiative]
[add more rows as necessary]	[add more rows as necessary] 

PART 4: STORAGE

22. Is all Personal Information involved in your initiative stored within standard Camosun College storage locations, technologies, or services?

☐ Yes ☐ No

Camosun College storage: Please list the approved standard Camosun College storage locations, technologies, and/or services.

- ☐ Microsoft 365 (SharePoint, OneDrive, Teams)
☐ Colleague
☐ D2L
☐ Team Dynamix
☐ Other: _____

Local Servers (and/or Systems):

- ☐ Vendor's Local Storage Option – please specify: _____
☐ Camosun College's Networked Drives
☐ Physical Media

Cloud Hosting:

- ☐ Vendor's Cloud Storage Option – please specify: _____

23. Is any Personal Information involved in your initiative stored outside of Canada?

☐ Yes ☐ No

24. Where is the Personal Information stored? Please identify applicable geographic locations for primary storage and backups. If Personal Information is stored in more than one primary location, the Privacy Office can expand the response field in this question.

Primary Storage

City (if applicable):
Province, Region, or State:
Country:

Back-up Storage (if applicable)

City (if applicable):
Province, Region, or State:
Country:

25. Does your initiative involve Sensitive Personal Information? (Any Personal Information can be Sensitive Personal Information in different contexts. Please contact the Privacy Office to discuss.)

☐ Yes ☐ No

26. Is any of the Sensitive Personal Information stored outside of Canada?

☐ Yes

☐ No

27. Where is the Sensitive Personal Information stored? Please identify applicable geographic locations for primary storage and backups. **Type N/A in the cells on the first row if Sensitive Personal Information is not stored outside of Canada as indicated in Question 26.**

Name of Third Party	Name of cloud infrastructure and/or platform provider(s) (Vendor's Cloud Storage option)	Where is the Sensitive Personal Information stored (including backups)?

PART 5: DISCLOSURE

FIPPA sets out requirements and restrictions related to disclosure of Personal Information. This section will help identify the legal authority for **disclosing** Personal Information, and consider risks related to that disclosure. **Fill out this section if Question 26 was answered "Yes"**

Complete this section if you are disclosing Sensitive Personal Information to be stored outside of Canada. You may need help from the Privacy Office.

28. Is any Personal Information being disclosed outside of Canada under FIPPA section 33(2)(f)? This section allows for information to be made available to the public under an enactment that authorizes or requires the information to be made public.
- ☐ Yes ☐ No
29. Is any of the Personal Information being disclosed outside of Canada under FIPPA section 33(2)(p)? This section allows disclosure for the purposes of (i) a payment to be made to or by Camosun College, (ii) authorizing, administering, processing, verifying, or cancelling a payment, or (iii) resolving an issue regarding a payment.
- ☐ Yes ☐ No
- ☐ The payment processor is out of scope of this PIA

30. Describe the privacy risks for disclosure of Personal Information outside of Canada.

Use the table to indicate the privacy risks. For each privacy risk you identify, describe the potential impact to individuals or Camosun College, and describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the Sensitive Personal Information (contractual, physical, technical, administrative measures) you outline elsewhere in this PIA. Privacy risks below are examples only; add new rows if necessary.

The risk of potential privacy breaches based on this initiative would be considered High (based on the UBC PIA classification tool). However, this risk can be managed and mitigated to acceptable levels by the implementation of adequate controls.

The following table consolidates key privacy and security risks associated with Microsoft Copilot Chat at Camosun College, along with mitigation measures.

Risk Category	Description	Impact	Likelihood	Mitigation Measures	Residual Risk
Personal Data Exposure	Users may input sensitive personal data into prompts, risking exposure if uploaded.	High	Medium	- Issue a directive on what should not be uploaded.	Low

	Includes oversharing and inadvertent disclosure. Example: An HR assistant asks Copilot to summarize “employee complaints.” Copilot pulls from a sensitive HR folder the assistant had access to by mistake, revealing personal info, legal notes, and termination records.			- Advise users to avoid entering sensitive personal data. - Users are instructed to verify that commercial data protection is in place when logged in with their Camosun credentials by confirming there is a green shield icon next to their user profile icon and name at the top of the application. - Incident management process for any data breach.	
Unauthorized Access	Weak credentials or system access could allow misuse of Copilot, exposing emails or files. Old or overly broad sharing (like “Everyone” or “All Employees”) means Copilot might surface sensitive data long forgotten.	Medium	Low	- Enforce Multi-Factor Authentication (MFA) and individual accounts. - Use Microsoft Entra ID for role-based access controls.	Low
Cloud and Configuration Vulnerabilities	Misconfigured settings or cloud attacks could expose data. Includes new attack surfaces from expanded access via prompt injection attacks. Malicious prompts could coerce Copilot into revealing confidential information or behaving unexpectedly – such as sending Phishing emails.	High	Low	- Consider Office 365 settings for maximum privacy and security. - Use Microsoft Defender for	Low

				real-time monitoring.	
Generative AI tools access personal information of other users to generate responses and/or train foundational LLMs.	Potential exists for our Microsoft 365 tenant to unintentionally leak between users, groups, and tenants. Since Copilot accesses data based on a user's permissions, if those permissions are too broad, Copilot can inadvertently expose sensitive information.	Medium	Low	- Copilot Chat presents only data that each individual can access through the same access controls used in other Microsoft 365 services. - Per the contractual terms and protections, no information from user interactions is used to train foundational LLMs. - Review changes to Microsoft disclosure of terms.	Low

Notes

AI-Specific Risks: AI inaccuracies are addressed through training, regular security updates, and guidelines prohibiting sensitive inputs.

PART 6: PROTECTION

Please share how the initiative will secure Personal Information to protect personal privacy. People, organizations, or governments outside of your initiative should not be able to access the Personal Information you collect, use, store or disclose. You need to make sure that the Personal Information is safely secured in both physical and technical environments.

31. Does your initiative involve digital tools, databases, or information systems?

☐ Yes ☐ No

32. What **physical security** safeguards are in place to protect Personal Information in this initiative?

Identify the elements of physical security that protect where the records for your initiative are stored (Check all that apply. Specify, "Other" if applicable)

Safeguard	At Camosun	At Third Party
Restricted access to property (i.e., key card access)	☐	☐
Security monitored building	☐	☐
Key locks and door astragals	☐	☐
Locked filing cabinets	☐	☐
Chain of custody process	☐	☐
"Clean desk" practices	☐	☐
Security officers	☐	☐
Security cameras	☐	☐
Other:	☐	☐

33. What **technical security** safeguards are in place to protect Personal Information in this initiative?

Describe the elements of technical security that protect where the records for your initiative are stored (e.g. secure passwords, encryption, firewalls, etc.) (More options on the following page)

Safeguard	At Camosun	At Third Party
Authentication control: Strong Password Management	☐	☐
Authentication control: Multi Factor Authentication ("MFA")	☐	☐
Role-based access	☐	☐
Encrypted in transit	☐	☐
Encrypted at rest	☐	☐
Isolation Control: Application	☐	☐
Isolation Control: Network	☐	☐
Isolation Control: Database	☐	☐
Vulnerability Scanning	☐	☐
Vulnerability Penetration Testing	☐	☐
Secure Configuration Management	☐	☐
Patch Management	☐	☐
Technical control: Perimeter firewalls	☐	☐
Technical control: Web application firewalls	☐	☐
Technical control: Denial of Service Mitigation	☐	☐
Technical control: Intrusion Detection and Prevention Systems	☐	☐

34. What administrative safeguards are in place to protect Personal Information?

Describe the elements of administrative security that protect where the records for your initiative are stored (e.g. aliasing, aggregation, policies/procedures, standards of practice, etc.)

Safeguard	At Camosun	At Third Party
Agreement/Contract	☐	☐
Privacy/Data Protection Policy	☐	☐

Documented business practices and processes for proper collection and management of Personal Information	☐	☐
Privacy training specific to the initiative	☐	☐
Cybersecurity Training	☐	☐
Staff Security Awareness Training	☐	☐
Dedicated Information Security Staffing	☐	☐
Information Security Policy	☐	☐
Vendor Third Party Compliance and Certifications (i.e., ISO, SOC Type 2, CSA, PCI DSS, SOX)	☐	☐
Security Incident Response Plan	☐	☐
Camosun College – Standards of Conduct Policy O-5.1.1 [employees]	☐	
Camosun College – Protection of Privacy Policy O-6.1	☒	
Camosun College – Systems and Networks Administration O-1.2	☐	
Camosun College – Acceptable Technology Use Policy O-1.1 [network use]	☐	
Camosun College – Academic Integrity Policy E-1.13 [students]	☐	
Camosun College – Student Misconduct Policy E-2.5 [students]	☐	
Other:	☐	☐

35. If the initiative involves a Third Party, please indicate what type of Agreement governs the relationship between Camosun College and the Third Party. Please select one.
- ☐ Camosun College GSA (negotiated Agreement between Camosun College and the Third Party)
 - ☐ Vendor's Agreement (negotiated Agreement between Camosun and the Third Party)
 - ☐ Online "Terms of Service" or "Terms of Use" (often non-negotiable)
 - ☐ Memorandum of Understanding/Memorandum of Agreement ("MOU"/"MOA")
 - ☐ Other (specify):
 - ☐ No Agreement
36. If the initiative involves a Third Party, does an End User License Agreement ("EULA") apply to the individuals whose Personal Information is involved?
- ☐ Yes ☐ No
37. The Privacy Officer will need to review all draft/proposed Contracts/Agreements (and related materials, i.e. contract appendices/schedules; Third Party privacy policies or online terms and conditions, if any) involved in the initiative. Have you ensured these have been provided? Check only one.
- ☐ Yes ☐ No ☐ N/A (No Third Party involved)
38. Where are the privacy related terms referenced in the contract or agreement if applicable? (Check all that apply)
- ☐ In the body of the contract or agreement
 - ☐ Third Party will sign Camosun College's Privacy Protection Schedule
 - ☐ Third Party will sign Camosun College's Data Security Schedule
 - ☐ In the Third Party's privacy or data protection policy or appended schedules
 - ☐ In a separate Information Sharing Agreement

- ☐ There are no privacy related terms in the contract or agreement (or related documentation)
- ☐ There is no contract or agreement for this initiative

39. Controlling and tracking access

Review each strategy below that describes how to limit or restrict who can access Personal Information and how to keep track of who has accessed Personal Information in the past. Check all that apply. Specify "Other" if applicable.

- ☐ Managed role-based access to Personal Information for Camosun College employees
- ☐ Managed role-based access to Personal Information for Third Party
- ☐ Third Party access is time limited for installing, implementing, maintaining, repairing, troubleshooting, or upgrading an electronic system
- ☐ Third Party access escorted by authorized Camosun College employee
- ☐ Audit logs at Camosun College
- ☐ Audit logs from Third Party
- ☐ Other: *(fill in details)*

40. Artificial Intelligence ("AI"): Are you aware whether this initiative actively incorporates or uses any AI features? If yes, please contact the Camosun College Privacy Office at privacy@camosun.ca.

- ☐ Yes ☐ No ☐ Unknown

PART 7: ACCURACY AND CORRECTION

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's Personal Information is accurate and complete. FIPPA also gives an individual the right to request correction of errors or omissions to their Personal Information.

In this section, please demonstrate how you will make a reasonable effort to ensure the Personal Information you have on file is accurate and complete.

41. How will Camosun College ensure that the Personal Information is accurate and complete? (Check all that apply)

- ☐ Individuals input their own Personal Information
- ☐ Individuals update their own Personal Information
- ☐ Employee verifies that information is accurate and complete before processing
- ☐ Documented processes to ensure accurate and complete data entry and maintenance
- ☐ The Third Party manages the accuracy and completeness of Personal Information under the direction of Camosun College
- ☐ Software or service uses automated processes to enter and manage Personal Information
- ☐ Other: *(fill in details)*
- ☐ Other: *(fill in details)*

42. Is there a documented process in place to correct Personal Information?
- ☐ Yes ☐ No
43. Sometimes it is not possible to correct the Personal Information. FIPPA requires a process to make a note on the record about the request for correction if it isn't possible to correct the record itself. Is there a documented process in place to annotate the record?
- ☐ Yes ☐ No ☐ N/A (Corrections possible)
44. If there is a request for correction from an individual and Camosun College or the Third Party disclosed that individual's Personal Information in the last year, FIPPA requires that Camosun College or the Third Party provide the applicable other public body or Third Party about the request for correction. Will Camosun College or the Third Party ensure that these notifications are done when necessary?
- ☐ Camosun College will forward correction notifications
- ☐ Third Party will forward correction notifications
- ☐ Camosun College and Third Party will split responsibility based on who was authorized to disclose Personal Information to third parties before a correction request was made.

PART 8: RETENTION AND DISPOSITION

FIPPA requires that public bodies keep Personal Information for a minimum of one year after it is used to make a decision. Personal Information needs to be disposed of to limit privacy risk after legal retention timelines.

- 45.** How long will Camosun College need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.

Record Type:	Retention Period (in years/months):
Record Type:	Retention Period (in years/months):
Record Type:	Retention Period (in years/months):
Record Type:	Retention Period (in years/months):

- 46.** How long will the Third Party need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.

Record Type:	Retention Period (in years/months):
Record Type:	Retention Period (in years/months):
Record Type:	Retention Period (in years/months):
Record Type:	Retention Period (in years/months):

- 47.** How will you ensure that the records containing Personal Information are disposed of in accordance with the retention schedule noted in questions above? (Check all that apply)

- ☐ Schedule records review and disposition dates in Outlook calendars
- ☐ Build conditions for disposal into department Standard Operating Procedures
- ☐ Send direct written communication to staff or service providers.
- ☐ Other (explain):

- 48.** What methods will be used to dispose of Personal Information following retention period? (Check all that apply.)

- ☐ Camosun College business unit shredding on campus
- ☐ Camosun College contracted shredding service provider
- ☐ Camosun College deletion of electronic record(s)
- ☐ Service Provider shredding/deletion of record(s) under Camosun College contract
- ☐ Service Provider shredding/deletion of record(s) under Camosun College written instruction
- ☐ Other (explain):
- ☐ Other (explain):

PART 9: INFORMATION FLOW

49. Complete the Information Flow Table

Use column 1 to describe the way Personal Information moves through your initiative step by step. Describe the steps as if you were explaining it to someone who does not know about your initiative.

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of Personal Information.

The Privacy Officer will complete column 3 to identify the legal authority you have for the collection, use or disclosure.

Information Management Steps	Collection, use or disclosure	PIPPA and other legal authorities
Step 1:		
Step 2:		
Step 3:		
Step 4:		

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

PART 10: TRAINING

50. Identify which of the following activities all employees and Third Party (as applicable), will be trained on when collecting and managing the Personal Information for the College initiative.
- ☐ Collection: Limit the collection to only what is explicitly necessary
 - ☐ Use: Use the Personal Information only for the purpose for which it was originally collected
 - ☐ Access: Only authorized employees (and, where applicable, service providers) may access the Personal Information
 - ☐ Disclosure: Not to disclose the Personal Information inside or outside Camosun College unless authorized under FIPPA
 - ☐ Storage: To store the Personal Information only in Camosun College-provided or approved storage locations and not to store unnecessarily in multiple locations
 - ☐ Retention: to keep the Personal Information for a minimum of one year – with longer retention periods only when necessary
 - ☐ Disposal: To dispose, when applicable, in a secure method that renders the Personal Information permanently irretrievable

PART 11: PERSONAL INFORMATION BANKS

51. Will your initiative result in a Personal Information Bank ("PIB")? A PIB is a collection of Personal Information searchable by name or unique identifier. If yes, please complete the table below. If more than one PIB will result, copy and paste an additional copy of the table below and fill out a separate table for each PIB.
- ☐ Yes ☐ No

Title	
Location	
Personal Information Types	
Categories of Individuals Included	
Collection Authority	
Purpose of Personal Information	
Categories of Persons Managing Information	

PART 12: OIPC REVIEW REQUIREMENTS (Privacy Officer to Complete)

52. Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, this PIA must be submitted to the Office of the Information and Privacy Commissioner.
- ☐ Yes ☐ No
53. Is this initiative a common or integrated program or activity? If this PIA addresses a common or integrated program, this PIA must be submitted to the Office of the Information and Privacy Commissioner.
- ☐ Yes ☐ No

PART 13: PRIVACY OFFICE(R) COMMENTS

This PIA is based on a review of the material provided to the Privacy Office(r) as of June 16, 2025. If, in the future, any substantive changes are made to the scope of this PIA, the College will have to complete a PIA Update and submit it to Privacy Office(r).

Privacy Office Signature

This PIA is based on a review of the material provided to the Privacy Office as at the date in Part 13 Privacy Officer Comments above.

Name and Title	Signature	Date signed
Ann Behennah, Privacy Officer	Ann Behennah	June 16, 2025

PART 14: APPROVAL SIGNATURES

Institution Signatures

This PIA is compliant with FIPPA when it accurately documents information management practices and information flow at the time of signing. If there are any changes to the overall initiative, including to the way Personal Information is collected, used, stored, or disclosed, the Department will inform the Privacy Office, and if necessary complete a PIA update.

By signing where required below, the signatories acknowledge and confirm their declarations as noted.

Declaration of Initiative Lead: I confirm that I understand the privacy impacts of this College initiative and I am committed to my FIPPA obligations related to the collection and management of Personal Information involved in the initiative. If there are any changes to the initiative, including to the way Personal Information is collected, used, stored, or disclosed, I understand that the department will need to inform the Privacy Office and if necessary, complete a PIA update. I will establish and document information management guidelines for the Personal Information and ensure these are followed. I will ensure employees are trained on and able to comply with their obligations under FIPPA; related College policies and procedures; and Camosun College Privacy Office recommendations relative to this initiative.

Signature of Initiative Lead or PIA Drafter

Name and Title	Signature	Date signed
Sybil Harrison Interim Associate Vice-President Education and Innovation	Section 22	June 16, 2025
Evan Hilchey Interim Associate Vice-President Administration		June 24, 2025

Declaration of Dean / Director / Budget Holder/ WPL/ One-Over-One Signatory: I confirm that I have reviewed this PIA and I acknowledge the residual privacy risks identified. I support the department by providing financial, time and operational resources to comply with FIPPA, related College policies and procedures and Camosun College Privacy Office recommendations relative to the initiative.

Signature of Dean / Director

Name and Title	Signature	Date signed

Declaration of Information Security: (Required only when college initiative involves Information Security considerations).

I confirm that I am satisfied that the Information Security safeguards employed in this college initiative meet reasonable requirements relative to the amount or sensitivity of the Personal Information or Camosun College business information described in this PIA.

Signature of Information Security

Name and Title	Signature	Date signed
Farzaan Nusserwanji	<i>fnusserwanji</i>	2025-06-05

Declaration of Information Technology: (Required when College initiative involves use of Camosun College IT systems or integration of Third-Party technology with Camosun College IT systems.)

I confirm that I understand and approve of the proposed use-case of Camosun College IT systems described in this PIA, where applicable. I understand and approve of the Third Party's integration with Camosun College's IT systems for the College initiative described in this PIA, where applicable.

Signature of Information Technology

Name and Title	Signature	Date signed
Ted Pennell Chief Information Officer		

Declaration of Head of Public Body or Designate: (Required where proportionate to the sensitivity of the personal information and/or the risks of the initiative). **NOT APPLICABLE**

I have reviewed this PIA carefully and accept and will be accountable for the residual privacy risks identified for this college initiative. I am satisfied with the completion of this PIA under FIPPA.

Signature of Head of Public Body or Designate Under FIPPA

Name and Title	Signature	Date signed