Privacy Impact Assessment

PIA - 25-06 Copilot

Legislative Requirement

Under section 69(5.3) of FOIPPA, UNBC is required to conduct a privacy impact assessment (PIA) and must do so in accordance with the directions of the Minister responsible for the Act.

A PIA needs to be conducted
- For a new initiative for which no PIA has previously been conducted.
- Before implementing significant change to an existing initiative, including but not limited to a change in the location in which sensitive personal information is stored.
- At the discretion of the person(s) with delegated authority under section 66 of the Act.

1. Accountability and Overview

1.1 Identify the department, unit, or program area involved in the initiative

All departments and faculties will have access to copilot

1.2 Identify the UNBC role responsible for the initiative

Chief Information Security and Privacy Officer is responsible for defining authorized data sets and uses.

1.3 Describe the governance model - who is accountable for the initiative

Chief Information Officer is responsible for provision access and managing the system.

1.4 List any relevant or previously completed PIAs

M365 PIA

1.5 List any relevant contracts, agreements, or software purchases

Be sure to follow any Contracts and Supply Chain Management requirements as set out in the Purchasing Policy

Microsoft 365 Contract

1.6 Describe the new initiative or change including the purpose, goals, and objectives
The purpose of this PIA is to define the conditions under which the use of Copilot is appropriate for UNBC controlled information.

1.7 List all interested parties impacted or involved	
Office of Data Governance, Privacy, and Information Security	Responsible for defining the scope of Copilot use and generating informational resources.
Office of the Chief Information Officer	Responsible for managing Microsoft 365, provisioning and deprovisioning access, and generating informational resources.
Faculty and Staff	Use Copilot in line with the scope defined in this PIA.

1.8 Timeline for the initiative		
Will this be an ongoing initiative or a one-time event with a defined end date?	Anticipated start date	Anticipated end date (if applicable)
✔ **Ongoing** ☐ **One-time**	2025-04-22	

2. Information and Uses in and out of Scope

2.1 Information and uses in scope

In scope data elements	FOIPPA Authorization	In scope uses	FOIPPA Authorization
Teams meeting.	s. 26(c)	Using Copilot to generate a Teams meeting summary is in scope.	s. 32(a)
Meeting materials.	s. 26(c)	Using Copilot to summarize meeting materials is in scope.	s. 32(a)
Draft policy or procedure document.	s. 26(c)	Using Copilot to assist in generating or refining a draft or suggest changes to an existing draft is in scope.	s. 32(a)
Lecture slides, teaching materials, or course syllabi.	N/A	Lecture slides, teaching materials, and course syllabi do not fall under FOIPPA. Copilot use is cautioned due to IP concerns.	N/A
Research materials.	N/A	Research materials do not fall under FOIPPA. Copilot use is dependant on REB requirements.	N/A
Website content.	s. 26(c)	Using Copilot to assist in generating or refining website content is in scope.	s. 32(a)
Completable forms.	s. 26(c)	Using Copilot to assist in generating or refining a completable form is in scope.	s. 32(a)
See Appendix 1 for more information	N/A		N/A

2.2 Systems, records, and information sets in scope

Information and records that are stored in the Microsoft 365 environment (Teams, Outlook, SharePoint, etc.) or involve Microsoft products (Word, Excel, PowerPoint) and do not contain sensitive personal information, are in scope.

2.3 Data classification of information in scope

Public and internal information. See Appendix 2 for definitions.

2.4 Information and uses out of scope

Out of scope data elements	FOIPPA Authorization	Out of scope uses	FOIPPA Authorization
Job applicant resumes or CVs.	N/A	Inputting resumes or CVs into Copilot in order to make hiring decisions is out of scope.	N/A
Faculty tenure and promotion applications and supporting documents.	N/A	Inputting faculty tenure and promotion applications into Copilot in order to make decisions about tenure is out of scope.	N/A
Student papers or assignments.	N/A	Inputting student papers or assignments into Copilot in order to assign a grade or determine if AI had been used is out of scope.	N/A
Employee performance reviews.	N/A	Inputting employee performance reviews into Copilot in order to make decisions about raises, promotions, or termination is out of scope.	N/A
Prospective student applications to UNBC.	N/A	Inputting prospective student application into Copilot in order to make admission decisions is out of scope.	N/A
Request for Proposal submissions.	N/A	Inputting RFP submissions into Copilot in order to determine what bid to award a contract to is out of scope.	N/A
Report generated using Banner or Moodle information.	N/A	Inputting information stored in Banner or Moodle is out of scope.	N/A
See Appendix 1 for more information.	N/A		N/A

2.5 Systems, records, and information sets out of scope

Information stored in Banner, FAST, Moodle, and other non-Microsoft information systems cannot be used in Copilot. Information sets containing sensitive personal information, confidential third party business information, and confidential financial information cannot be used in Copilot.

2.6 Data classification of information out of scope

Confidential and restricted information. See Appendix 2 for definitions.

5. Storage of Personal Information

5.1 Does the initiative involve digital tools, databases, or information systems?

☑ Yes ☐ No

If yes, contact Information Security to determine whether the initiative requires a security and threat risk assessment.

5.2 As part of this initiative, will personal information be stored outside of Canada?

☑ Yes ☐ No

5.3 Describe how information will be stored during this initiative

Cloud storage, SaaS, G Drive, etc.

All information generated by Copilot will remain in the Microsoft 365 environment. Microsoft 365 does store Canadian client information in Canadian data centers, though information can be accessed and backed up outside of Canada.

6. Disclosure of and Access to Personal Information

6.1 Does the initiative involve disclosing information to third parties (non-UNBC employees)?

☐ Yes ☑ No

6.2 Provide details on the disclosure, including to whom, purpose, method of disclosure, and how personal information will be stored by the third party. Add extra information for disclosure outside of Canada.

Information entered into Copilot is not used to train the AI model.

6.3 Does the initiative involve providing contractor(s) access to UNBC managed systems?

Access to Outlook, Banner, FAST, etc.

☐ Yes ☑ No

If yes, privacy and security requirements for contractor access will be defined in section 10, Safeguards.

Using **COPILOT** at UNBC

Copilot is Microsoft's AI assistant aimed at boosting productivity by offering intelligent support and insights across various tasks. However, it's important to note that it may not be suitable for every situation, as generative AI can produce biased or inaccurate outputs. Always verify the information provided by Copilot before using it.

Think about using Copilot as a 3-step process

YOU INPUT A PROMPT

COPILOT OUTPUTS A RESPONSE

YOU CHOOSE TO USE THE OUTPUT OR NOT

You have a choice over inputs and how you use generated outputs

ACCEPTABLE INPUTS

- Publicly available web content
- Your own intellectual property
- General questions and queries
- Public UNBC records

INPUTS TO AVOID

- Personal information
- Student assignments
- Applicant resumes
- Contracts with third parties
- Confidential infomation

VALID USES

- Summarize meeting recordings
- Organizing your schedule
- Developing initial drafts
- Developing teaching material

INVALID USES

- Making hiring decisions
- Evaluating employee performance
- Evaluating student assignments
- Analyzing personal information

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Information and Record Classification Levels

	Restricted	Confidential	Internal	Public
	Very sensitive information Breach reasonably expected to result in significant harm	Sensitive information Breach may result in significant harm	Not sensitive information Breach not likely to result in significant harm	
Definition	Highly sensitive information or records that require additional protective safeguards	Sensitive business or personal information.	Information or records that are used by a unit within UNBC, and not approved for distribution outside of the University.	Factual information or records that have been approved for public release.
Examples	Wellness records, banking information, student appeals, etc.	Student records, employee evaluations, employee records, etc.	Meeting notes of informal meetings, planning documentation, general email correspondence, etc.	Promotional materials, information on UNBC website, syllabi, etc.
Recommended Management of Information	Access to information is role-based, and limited to those roles that require the information to complete their operational duties. Stored within a controlled-access system (e.g., password protected, locked filing cabinet). Routinely audit user access.	Access to information is role-based, and limited to those roles that require the information to complete their operational duties. Stored within a controlled-access system (e.g., password protected, locked filing cabinet).	Access is limited to employees and authorized users for business-related purposes.	Proactively provide this information to the public in a convenient way.