College of New Caledonia
CNC

Privacy Impact Assessment

Microsoft 365

PIA#21-006

Table of Contents

PART 1: GENERAL INFORMATION

Initiative title:	Microsoft 365
Organization:	College of New Caledonia
Branch or unit:	Information Technology Services
Your name and title:	[redacted] Business Analyst Consultant - [redacted] 22(1) Jo-Ann Bellamy, Hooper Access and Privacy Ltd. - [redacted] 22(1)
Your email:	[redacted] 22(1) jbellamy@hooperconsulting.ca
Initiative Lead name and title:	David Lampron Chief Information Officer
Initiative Lead phone:	250- 561-5812

Initiative Lead email:	Lamprond1@cnc.bc.ca
Privacy Officer:	David Loewen
Privacy Officer phone:	(250) 562-2131 ext. 5626.
Privacy Officer email:	loewend7@cnc.bc.ca

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Related PIAs, if any:
None

1. What is the initiative?

The current set of communication and collaboration tools that CNC is using are becoming outdated and unsustainable. Upgrades to existing on premise solutions will require considerable time and human resources detracting from the ability for CNC Information Technology Services ("ITS") to meet the demands of CNC students, faculty, and staff. ITS is proposing the adoption of the Microsoft 365 platform to facilitate collaborative communication technologies and support high quality and agile academic delivery.

This privacy impact assessment will cover the following products: Office ProPlus, Teams, Sway, Exchange Online, Sharepoint Online with OneDrive, and Azure Active Directory Fabric Services. This PIA covers A3 License Features available as of November 2021. The option exists to move to A5 licensing for more security features which will be evaluated in future addendums.

All faculty, staff, administrators, and students will use M365. Any alumni, researchers, visiting scholars, and external consultants that are provided access to any office productivity software

at CNC will be using M365. All faculty, staff, students, alumni, donors, vendors, consultants, and other payees will have at minimum identity information managed in Azure Active Directory.

Overview of Microsoft 365

Microsoft 365 consists of:

1. Office ProPlus (desktop and cloud-based traditional Microsoft suite of software)
2. Exchange email and Teams (which includes audio and video conferencing, Sway services, Voice over IP, etc.)
3. Microsoft 365 SaaS fabric services (security and compliance management tools that overlay all application services)
4. OneDrive (cloud based personal file storage)
5. SharePoint (Web-enabled collaboration services)

Supporting Microsoft 365 is a web-based administrative interface that allows users to configure settings delegated to them by client administrators. In this way, both administrators and individual users can utilize privacy and security protections and preferences available to them. For example, administrators can restrict the domains that are permitted to interact with a service, and the users can further limit this as necessary. Program areas with particularly sensitive data may add additional safeguards. See the information documented under the questions in Part 3 of this PIA for more details.

Azure Active Directory (AAD)

Azure Active Directory supports Microsoft 365 by providing an identity and access management service. It combines core directory services, identity governance and application access management. Azure Active Directory is a modern identity management solution spanning on-premises and cloud, providing the necessary security capabilities for application access control, federation, identity management, user provisioning, information protection, standard protocols support, comprehensive development libraries, and more.

Azure Rights Management Service

Azure Rights Management Service intends to protect information at the data level using encryption, user identity, and authorization policies to help secure files and email in transit across multiple devices—phones, tablets, and PCs. This service allows CNC to encrypt shared data and apply policies on data to limit or allow actions by the recipient of the data.

Exchange Online

Microsoft Exchange Online is an email, calendar and contacts solution delivered as a cloud service, hosted by Microsoft. Exchange Online provides end users with a familiar email experience across PCs, the Web, and mobile devices, while giving CNC IT administrators web-based tools for managing their online deployment.

Exchange Online Protection (EOP)

Exchange Online Protection is the enterprise-class spam and malware filtering service offered in conjunction with Exchange Online. EOP can utilize layers of protection features deployed across

a global network of data centres, simplifying the administration of messaging environments; however, for the purposes of CNC, EOP will be deployed only through Canadian data centres.

Teams

Teams is an instant messaging client with audio and video chat capabilities. The real-time communications server software provides the infrastructure for enterprise instant messaging, presence, VoIP, ad hoc and structured conferences (audio, video, and web conferencing) and public switched telephone network (PSTN) connectivity through a third-party gateway or SIP trunk.

SharePoint Online

SharePoint Online, part of the Microsoft 365 suite for online productivity solutions, and the successor to Business Productivity Online Services (BPOS), provides a platform for CNC to enhance and extend the functionality of existing on-premises SharePoint deployments using a cloud-based service. SharePoint Online provides a single, integrated location where people can:

- Collaborate with team members and external parties,
- Find organizational resources,
- Look up corporate information, and
- Glean business insights for better-informed decisions.

OneDrive for Business

OneDrive for Business is an integral part of Microsoft 365 and is provided by Microsoft 365's SharePoint Service. It provides a secure cloud storage location where employees can store, share, and sync their work files. OneDrive allows employees the ability to easily share files between their different devices.
Microsoft 365 (M365) is a software-as-a-service (SaaS) product. M365 was selected as the optimal choice because Microsoft operates datacenters for the services CNC would like to utilize that are hosted in Canada.
Provided the appropriate safeguards, authentication, and logging are in place, CNC will be able to work with Microsoft to enable and empower the employees and students to achieve better outcomes with a better experience.

2. What is the scope of the PIA?

This PIA addressed the collection, use, disclosure, storage, and security of personal information in the Microsoft 365 products being used by CNC.

3. What are the data or information elements involved in your initiative?

P System or Service Data

System or Service Data is information about, and generated by, an information system or cloud service, and is non-personal in nature. Examples of service data include remaining storage capacity, system health indicators, network traffic volume and bandwidth consumption. All of these are examined or used solely for the purpose of providing the cloud service. System data is distinct from

CNC content and is used solely for the purpose of providing, operating, and maintaining the service, or diagnosing and/or troubleshooting in the event of problems or system outages.

Employee Contact Data

Employee Contact Data is information to identify and differentiate users of the cloud service. This includes User ID, Organizational ID, and basic user contact information (e.g., phone number or email address). This information is used by Microsoft staff to troubleshoot service and access issues (e.g., jsmith cannot access file A). Most of the Employee Contact Data is considered either non-personal information, or business contact information.

CNC Content Data

CNC user content consists of data, information, documents, spreadsheets, and other records that are authored, edited, communicated, maintained, and eventually disposed of by the user or ITS. For the purposes of analysis, user content is assumed to be, or assumed to contain personal information. Specific content will range in type, volume, and sensitivity according to the client activities in using Microsoft Cloud Services. CNC Content Data will not be stored in Microsoft Cloud Services outside of Canadian data centers.

Elements of User Data that will be synchronized with Microsoft Azure Active Directory

Our current configuration syncs all AD attributes from on-prem to Azure AD. However, we only populate a fraction of the attributes which are listed below. Additionally, there are metadata attributes which are used internally by AD and Exchange but are not directly populated by CNC. The following table includes information for both students and employees.

Attribute	*Description*
CN	*Common Name – Part of AD object identifier*
Description	*CNC stores Colleague ids in this field*
DisplayName	*<first name> <last name> (<username>)*
EmployeeId	*Colleague id*
EmployeeNumber	*Colleague id*
EmployeeType	*One of 'Employee' or 'Student'*
GivenName	*User first name*
HomeDirectory	*Path to on-prem personal file storage*
HomeDrive	*Drive letter for on-prem personal file storage*
HomeMDB	*On-prem exchange mail database name*
L	*City*
Mail	*CNC provided email address*
MailNickname	*CNC username*
Name	*CNC username*
SAMAccountName	*CNC username*
ScriptPath	*Path to local startup script*
SN	*User last name*
UserPrincipalName	*User principal name*

3.1 Did you list personal information in question 3?

Yes

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

5. Collection, use and disclosure

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1: Personal information is collected from students when they register with CNC, or from faculty/staff when hired	Collection	26(c)	
Step 2: User account for M365 is created	Use	32(a)	
Step 3: User securely logs in to M365 with their assigned credentials	Collection	26(c)	
Step 4: Login credentials (personal information) are used to authenticate the user to M365 via token requests to allow access	Use	32(a)	
Step 5: User access is granted to M365	Use	32(a)	
Step 6: Personal information may be included when using M365 functions including email, documents, etc.	Use	32(a)	

[redacted] 15(1)(l)

[redacted] 15(1)(l)

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

CNC provides notification when employees and faculty are hired and when students register with CNC.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

No

8. Does your initiative involve sensitive personal information?

No

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

N/A

- If yes, go to question 10
- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

Microsoft's Canadian data centers are located in Quebec City and Toronto. Across its business, Microsoft stores Customer Data at rest within certain major geographic areas (a "GEO"). Canada has been defined as a "GEO", meaning that for CNC's purposes, all customer created content will be resident within Canada.

System data is stored both inside and outside of Canada and is accessible by authenticated administrators both inside and outside of Canada. Its use is controlled and limited to the provisioning, maintenance, support, and ongoing operation of cloud services. System data does not contain any personally identifiable information.

CNC's Content Data will not be moved or copied to data centers outside Canada without CNC's explicit permission and technical authorization. This technical authorization is done by a process called Customer Lockbox, in short in the event that a Microsoft employee needs access to data owned by CNC in the course of troubleshooting then CNC M365 administration will have to give explicit permission to that technician in order to review the data/logs. This permission is time based and will automatically be revoked. A key premise of the model is that

the customer controls and owns their content, Microsoft has no standing access to the service components that CNC is responsible for (applications configurations, and all application data) in their cloud SaaS solution. Customer Lockbox functionality applies to the Microsoft 365 server applications: Exchange, Skype, SharePoint, OneDrive, and related services; as well as the Azure Service Fabric including the Azure Active Directory and related services.

After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider?

N/A

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
N/A		

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

N/A

13. Does the contract you rely on include privacy-related terms?

N/A

- If yes, describe the contractual measures related to your initiative.

15. What controls are in place to prevent unauthorized access to sensitive personal information?

N/A

16. Provide details about how you will track access to sensitive personal information.

N/A

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.
N/A					

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. 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.

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

Yes

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

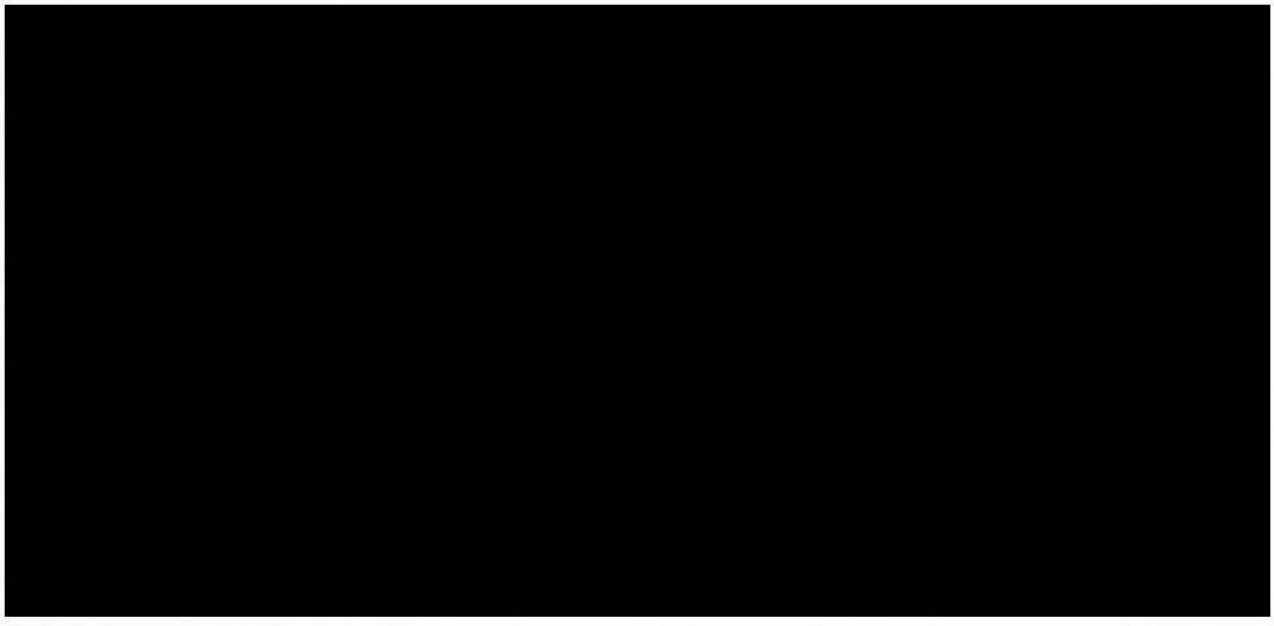
18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

Yes.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

CNC



15(1)(l)

M365

15(1)(l)

15(1)(l)

Information on physical security of Microsoft datacentres can be found at Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs

Information on technical security can be found at as follows:

Platform Security: Azure platform integrity and security - Azure Security | Microsoft Docs

Network Security: Network security concepts and requirements in Azure | Microsoft Docs

Data Security: Azure encryption overview | Microsoft Docs

Logging and Alerting: Azure security logging and auditing | Microsoft Docs

Information on technical and physical security for Microsoft 365 can be found at: https://docs.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	Yes

Strategy	
Employees that need standing or recurring access to personal information must be approved by executive lead	Yes
We use audit logs to see who accesses a file and when	See below
Describe any additional controls:	[redacted]

15(1)(l)

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Yes. Azure Active Directory, where attributes about users are kept, will have the data synchronized with the on-premise active directory at least once a day in the case of normal attributes. In the event of a changed password, [redacted] This is a fully automated process.

15(1)(l)

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A. Personal information will be updated daily as described in 22.1 above.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A. The personal information in this initiative will not be disclosed to any third parties.

23. Does your initiative use personal information to make decisions that directly affect an individual?

No.

- If yes, go to question 25
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

N/A

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

No.

- If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA

26. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

Yes. Azure Active Directory contains user profile information matching employees to appropriate access to information and information management controls within databases containing structured and unstructured data. This PIB is designed to track the activities of all users of CNC's M365 platform to ensure system compliance, security of information contained on CNC's instance of the M365 platform, and integrity of user access controls.

- If yes, please complete the table below.

Describe the type of information in the bank: User ID, name, type of user, last logon time, location of user, how user interacts with the system, job title, and direct supervisor. Type of user is separated into categories including Employees, Students, Alumni, Consultants, PostDoctoral Fellows, Contractors, Prospective Students, Visiting Scholars, and any other types of users that may need to be defined as users on the M365 platform in the future. Also see table in #3 that defines the attribute types that may be available in the PIB.
Name of main organization involved: College of New Caledonia
Any other ministries, agencies, public bodies, or organizations involved: None
Business contact title and phone number for person responsible for managing the PIB: Nick Sarabyn Manager, Information Architecture sarabynn@cnc.bc.ca 250-562-2131

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Add new rows if necessary.

Possible risk	Response
Risk 1: Unauthorized individuals at CNC could access the personal information in the system.	Access is based on need-to-know principles. [redacted] Employees must sign privacy and confidentiality agreement. See security information in #19 of this PIA.
Risk 2: Employee account is accessed externally by another individual.	Employee assigns their own unique password to protect their information and self manages changes. [redacted]
Risk 3: Employee personal information is compromised when transferred to the service provider (Microsoft).	All data is encrypted during transmission [redacted] Microsoft only has access to the data that CNC has authorized (based upon authorized and restricted need-to-know basis). See security information in #19 of this PIA.
Risk 4: Third party service providers (Microsoft) could access the personal information in the system.	Contractual agreement terms, obligations, and requirements. Third party service providers have internal security and privacy policies and protocols in place that ensure requirements and obligations are met (e.g., data access security protocols, Non-disclosure Agreements, etc.).

15(1)(l)

15(1)(l)

15(1)(l)

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Signature	Date signed
Privacy Consultant	Bev Hooper, Hooper Access and Privacy Consulting Ltd.	[redacted]	March 28/22

22(1)

Program Area Signatures

This PIA accurately documents the data elements 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 program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Signature	Date signed
Initiative lead			
Program/Department Manager			

Role	Name	Signature	Date signed
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate Only required if personal information is involved			