- Review of Office applications and Office for business servers or services administered by Capilano University IT Services.
- Review of Office applications and Office for business servers or services administered by Microsoft.
- Privacy controls as well as data flow between Windows 10 and the following Office 2016 applications:
  - Word
  - Excel
  - PowerPoint
  - Outlook
  - Access
  - Publisher
  - Skype
  - Office applications and non-Microsoft services

3. Related Privacy Impact Assessments

IT169 – iCAP 2018-2019 (Covers all student spaces using Windows 10 operating systems and Office 2016 software packages).

4. Elements of Information or Data

Windows 10 Elements

Cortana Personal Assistant:

Cortana learns about user activities by using data from the device, personal Microsoft account, third-party services and other Microsoft services. To enable Cortana to provide personalized experiences and relevant suggestions, Microsoft collects and uses various types of data, such as device location, data from the calendar, the applications used, data from emails and text messages, call history, contacts and other users who were interacted with on the device. Cortana also learns about users by collecting data about how the device is used and other Microsoft services, such as music, alarm settings, whether the lock screen is on, what is viewed and purchased, browsing and Bing search history, and more.

Cortana Location services:

Cortana regularly collects and uses current location data, location history, and other location signals (such as locations tagged on photos uploaded to OneDrive). This location data is used to provide the most

relevant notices and results and to make suggestions that help save time, such as traffic and location based reminders.

Cortana Text Messages and Email:

Cortana accesses user messages to do a variety of things such as: allowing event entries into the calendar, apprising users of important messages, and keeping updated information on events or other things that are important, like package or flight tracking. Cortana also uses messages to help with planning around events**.**

Cortana Communications History:

Cortana learns who is most important to the user from call, text message, and email history. This is used to keep track of people most relevant and preferred methods of communication, flag important messages and improve other Cortana services such as speech recognition.

Cortana Input Personalization:

This element enables the automatic learning component of input personalization that includes speech inking and typing. Automatic learning enables the collection of speech and handwriting patterns typing history contacts and recent calendar information. It is required for the use of Cortana. Some of this collected information may be stored on the user's OneDrive in the case of inking and typing; some of the information will be uploaded to Microsoft to personalize speech. Automatic learning for speech may not be available for all languages even when inking and typing is available.

https://privacy.microsoft.com/en-ca/windows-10-speech-inking-typing-and-privacy-faq

Online Speech Recognition:

[Amended December 2023 – Markus Polkki]

This setting allows users to "use their voice for dictation and other apps using Microsoft's online speech recognition technology." Accessibility Services has expressed interest in enabling this setting on student devices. Doing so allows students to toggle Online Speech Recognition for their profile on student devices they log into (off by default).

Per Microsoft's updated Privacy Policy there is an option to contribute voice clips to help improve the voice recognition service, which are "de-identified" as they are stored on Microsoft servers:

https://support.microsoft.com/en-us/windows/how-does-microsoft-protect-my-privacy-while-improving-its-speech-recognition-technology-f465d7a7-4a4f-40b7-9441-f0e6e97e24ec

Upon testing, however, there is no option to opt into this once managed through our policy. This was confirmed by monitoring the corresponding setting in the Registry and ensuring it was off and remained off with Online Speech Recognition enabled.

Cortana Automatic Learning:

This element enables the collection and storage of text and ink written by the user in order to help adapt handwriting recognition to the vocabulary and handwriting style of the user. Text that is collected includes all outgoing messages in Windows Mail and MAPI enabled email clients as well as URLs from the Internet Explorer browser history. The information that is stored includes word frequency and new words not already known to the handwriting recognition engines (for example proper names and acronyms). Deleting email content or the browser history does not delete the stored personalization data. Ink entered through Input Panel is collected and stored.

Cortana Microsoft Apps and Services:

Cortana uses data collected through other Microsoft services to provide personalized suggestions. For example, Cortana uses data collected by the MSN Sports app so it can automatically display information about the teams a user may follow. It also learns favorite places from the Microsoft's Maps app so it can offer suggestions.

Cortana Third-Party Services:

Cortana also allows the user to connect to third-party services for additional personalized experiences based upon data from the third-party service.   For example, choosing to sign into Facebook or LinkedIn within Cortana allows Microsoft to access certain Facebook or LinkedIn data so that Cortana and Bing can give personalized recommendations.

Cortana Browsing History:

If the user chooses to send their full browsing history to Microsoft in Microsoft Edge, Cortana can provide suggestions based on the sites visited in Microsoft Edge.

Cortana Search History:

User Bing search queries - even if Cortana does the searching - are treated like any other Bing search queries.

https://privacy.microsoft.com/en-ca/windows-10-cortana-and-privacy

Picture Password / Windows Hello:

This element allows you to control whether a domain user can sign in using a picture password instead of the traditional alpha, numeric or alphanumeric password.

Windows Hello takes the data from the face or iris sensor or fingerprint reader and creates a data representation—not an image; it's more like a graph that is then encrypted before it's stored on the device.

https://privacy.microsoft.com/en-ca/windows-10-windows-hello-and-privacy

Advertising ID:

This element is used to customize an online experience, some of the ads received on Microsoft websites and apps are tailored to your interests based on your previous activities, searches and site visits.

http://choice.microsoft.com/en-us/opt-out

Allow Windows Applications Access:

This element allows Windows applications access to the following information:

- Access to account information including name picture and other available information
- Access to call history
- Access to contacts
- Access to and send email
- Access to location
- Access to messaging
- Access to motion data
- Access to the calendar
- Access to the camera
- Access to the microphone
- Access to trusted devices
- Access to control radios such as Bluetooth
- Access to sync with devices such as Xbox, TVs and Projectors

https://privacy.microsoft.com/en-ca/windows-10-location-and-privacy
https://privacy.microsoft.com/en-ca/windows-10-camera-and-privacy

Application Telemetry:

This element is a mechanism which tracks anonymous usage of specific Windows system components by applications (these could be 3rd party application).

Microsoft Consumer Experience:

An example would be Twitter or Candy Crush (or other store applications) installing without the users knowledge based on location or other metadata.

Allow Telemetry:

Telemetry data is system data that is uploaded by the Connected User Experience and Telemetry component. The telemetry data is used to keep Windows devices secure, and to help Microsoft improve the quality of Windows and Microsoft services. Windows 10 telemetry settings applies to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10.

Feedback Notifications:

This element allows the user to provide feedback information to Microsoft.

Windows 10 – Microsoft Office Professional Plus 2016 Data Flow Elements

The following describes current data flows between Office 2016 applications for Windows 10 desktop and services, including data that flows from users, both home and business customers, to Microsoft services. Data from the Microsoft applications you install on a device goes to different Microsoft server and services (endpoints) and has different privacy controls.

There are different types of data flows starting with data that stays on the device and extending to data that flows from the device to Microsoft. The available privacy controls vary depending on where the data flows.

The data flow and privacy control information covered here applies to the following Office 2016 desktop applications:
- Word
- Excel
- PowerPoint
- OneNote

Common Data Flows Between the Office Applications and Windows 10:

Office applications and local device:
- Such as data stored on the device, such as local storage of a photo.

Office applications and Microsoft Services:
- Client data used by Microsoft cloud services, such as Smart LookUp, Translation and Bing Weather.

Office telemetry
- Microsoft uses this performance and usage data to help improve the quality of Office and Office services.

Office Professional Plus 2016 Data Flows Between the Office Applications and Windows 10:

Office applications and Office for business servers or services - Administered by CapU IT Services:

- IT administrators can advise users whether applications and services are operated by Microsoft or not. These servers are typically accessed using your work or school account. Some cloud services are essential to the application operation such as OneNote synchronization with the OneNote cloud service.

Office applications and Microsoft servers or services – Administered by Microsoft:

- The type of Office installation will either be subscription, such as Microsoft Office 365 Business or Microsoft Office 365 ProPlus, or non-subscription installations such as **Microsoft Office Professional Plus 2016** or Microsoft Office Standard 2016. These servers are typically accessed using your Organizational Account. Examples of the Office 365 cloud services include Licensing, Activation, OneDrive, and recently used documents. Some cloud services are essential to the application operation such as Outlook synchronization with the Exchange service.

Office applications and non-Microsoft services:

- IT administrators can advise users whether applications and services are operated by Microsoft or not. User data can flow to on-premises servers, such as servers running Exchange Server or SharePoint Server. Some on-premises services are essential to the application operation such as emails from Outlook to the Exchange Server

https://support.office.com/en-us/article/Data-flows-and-privacy-controls-for-Office-2016-a0a91b87-64b7-4554-bbe8-8a0b2d2230f0

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. **Storage or Access outside Canada**

   The Microsoft Privacy Statement best explains what personal data is collected and how it is used.   It should be assumed personal data is stored outside of Canada.

   In his blog post, "Privacy and Windows 10" Terry Myerson / Executive Vice President, Windows and Devices Group states "*With Windows 10, information we collect is encrypted in transit to our servers, and then stored in secure facilities.*"

6. **Data-linking Initiative***

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. **Common or Integrated Program or Activity***

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	No
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

* Please note: If your initiative involves a "data-linking initiative" or a "common or integrated program or activity", advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body's privacy office(r) to determine how to proceed with this notification and consultation.

For future reference, public bodies are required to notify the OIPC of a" data-linking initiative" or a "common or integrated program or activity" in the early stages of developing the initiative, program or activity. Contact your public body's privacy office(r) to determine how to proceed with this notification.

8. **Personal Information Flow Diagram and/or Personal Information Flow Table**

   By default users have the ability to change most of the features that will be disabled out of the box in order to improve their Windows 10 experience with the operating system and the Office 2016 suite of applications. Therefore all features that collect personal data will be disabled and locked down using Windows 10 polices or registry edits.

   A flow diagram or personal information table is not included as there will be no collection of personal information needed to demonstrate a flow or a populated flow table.

9. **Risk Mitigation Table**

   There are a number of features and products included in this initiative that can collect private information if users use them:

   Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Cortana – OS feature that collects private information in order to provide functionality*	*Will be disabled by Group policy and OS registry changes*	*None*	*High*
2.	*WiFi services – OS features that suggest open hotspots based on location*	*Will be disabled by Group policy and OS registry changes*	*None*	*Low*
3.	*Windows Hello and Picture password– OS features that allows the OS and application to recognize the user*	*Will be disabled by Group policy and OS registry changes*	*None*	*Medium*
	Online Speech Recognition	*Option to share voice clips with Microsoft will be disabled by Group policy..*	*None*	*Medium*
4.	*Advertising ID and access to language list – OS features that provide some information to applications and websites to improve usability*	*Will be turned off by Group policy and OS registry changes*	*Low*	*Low*

5.	*Account info access – OS feature that lets applications access the user's account information*	*Will be turned off by Group policy and OS registry changes*	*Low*	*Low*
6.	*Contacts – OS feature that allows applications to access the user's contacts*	*Will be turned off by Group policy and OS registry changes*	*Low*	*Low*
7.	*Location – OS feature that allows the OS, applications and services to access the user's location*	*Will be disabled by Group policy and OS registry changes*	*None*	*Medium*
8.	*Camera – OS feature that allows applications to use a camera, if one exists*	*On by default. The user can turn it off and select which applications can access it.*	*Low*	*High*
9.	*Microphone – OS feature that allows applications to use a microphone, if one exists*	*On by default. The user can turn it off and select which applications can access it.*	*Low*	*High*
10.	*Notifications – OS feature that lets applications notify the user audibly and visually*	*On by default. The user can turn it off*	*Low*	*Low*
11.	*Speech, Inking and Typing – OS features that allow the creation of a local user dictionary that makes better suggestions when using Cortana or Store applications*	*Will be turned off by Group policy and OS registry changes*	*Low*	*High*
12.	*Calendar – OS calendar feature that allows user to create calendar entries. Access to user's calendar by other apps can be permitted*	*Will be turned off by Group policy and OS registry changes*	*Low*	*Medium*
13.	*Call History – OS feature that allows applications to access the user's call history*	*Will be turned off by Group policy and OS registry changes*	*Low*	*Low*

14.	Email – OS feature that allows the OS and applications to send or access email	Will be turned off by Group policy and OS registry changes. The user can enable it and decide which applications can access email	Low	Medium
15.	Tasks – OS feature that allows applications to access the task feature	Will be turned off by Group policy and OS registry changes	Low	Low
16.	Messaging – OS feature that allows applications read and send text (SMS)	Will be turned off by Group policy and OS registry changes – The user can turn it on	Low	Medium
17.	Radios – OS feature that allows applications to send and receive data via Bluetooth of WiFi	On by default. The user can turn it off and select which applications can access it.	Low	Low
18.	Other devices – OS feature that allows for applications to share and sync info with wireless devices that don't explicitly pair	Will be disabled by Group policy and OS registry changes	None	No
19.	Feedback & Diagnostics – OS feature that collects data for improving experiences	Will be disabled by Group policy and OS registry changes	Low	Low
20.	Background applications – OS feature that allows application to run in the background	On by default. The user can turn it off and they can also individually turn off applications	Low	Low
21.	App diagnostics			
22.	Automatic file downloads			

10. Collection Notice

If your initiative is collecting personal information directly from individuals you must ensure that all individuals involved are told the following:

1. *The purpose for which the information is being collected*
2. *The legal authority for collecting it, and*
3. *The title, business address and business telephone number of an officer or employee who can answer questions about the collection.*

Please include your proposed wording for a collection notice and where it will be located for individuals to read before collection takes place. You can also attach a screen shot or a copy of your form where the collection notice would be located. For further help with collection notices please see the "Collection Notice Tip Sheet" located on the CIO's website.

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

11. **Please describe the physical security measures related to the initiative (if applicable).**

There is no change in the physical security of the workstations/laptops and it's out of scope for this initiative.

12. **Please describe the technical security measures related to the initiative (if applicable).**

All employee workstations will be encrypted with Bitlocker and each employee has its own Active Directory user account. The workstations are behind a firewall on a secure network and are protected with System Center Endpoint Protection by Microsoft as an antivirus.

13. **Does your branch/department rely on any security policies?**

Please describe any specific policies and procedures and provide contact details for someone who could answer further questions regarding these policies and procedures.

14. **Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.**

All users account are tide to security groups and the access is role based.

15. **Please describe how you track who has access to the personal information.**

The operating system in itself does not store personal information, and any access to personal information that would be facilitated by running the operating system is stored in other systems.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If**

personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

The information used by the operating system is maintained in Active Directory and the name of the user is only displayed if the workstation is locked so that the user is aware of the fact that his profile is active on the system.

17. **Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

    No

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

    For example: check to see that the information was obtained from a reputable source such as another government agency.

19. **If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

    If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please describe retention schedules that apply where retention exceeds the one year requirement of FOIPPA. Please contact your public body's privacy office(r) and/or records office(r) if you require assistance.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

No

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Privacy Office(r) Comments

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

Privacy Officer/Privacy Office Representative	Signature	Date

Privacy Impact Assessment for Non-Ministry Public Bodies

IT166 – Windows 10 and Office PP 2016 Migration

PIA#*[assigned by your privacy office(r)]*

Part 7 – Program Area Signatures

Program/Department Manager	Signature	Date

Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date

Head of Public Body, or designate	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

19