VANCOUVER ISLAND UNIVERSITY

PRELIMINARY PRIVACY IMPACT ASSESSMENTS

Microsoft Content Creation Apps:

- Editor
- Forms
- OneNote
- Publisher
- Sway
- Whiteboard

Version #:	V0.1 - Draft
Date:	March 28, 2023

INITIATIVE TITLE:	**Review of Microsoft Apps:** • **Editor** • **Forms** • **OneNote** • **Publisher** • **Sway** • **Whiteboard**
ORGANIZATION:	Vancouver Island University (VIU)
BRANCH OR UNIT:	IT
YOUR NAME AND TITLE:	Moira Connor, PrivacyWorks Consulting, Inc.
YOUR WORK PHONE:	778.388.2585
YOUR EMAIL:	moira@privacyworks.ca
INITIATIVE LEAD NAME AND TITLE:	Brad Moran, IT Business Architect, Vancouver Island University
INITIATIVE LEAD PHONE:	250.753.3245
INITIATIVE LEAD EMAIL:	Brad.Moran@viu.ca
PRIVACY OFFICER:	Bill Boyte
PRIVACY OFFICER PHONE:	250.740.6554
PRIVACY OFFICER EMAIL:	FIPPA@viu.ca

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:
• **Microsoft Office 365** • **Microsoft BI** • **Microsoft Bookings**

VERSION CONTROL

Date	Version	Author(s)	Version Notes
March 28, 2023	Draft	Moira Connor Use of Province of BC, PIA template for non-ministry public bodies.[1]	Initial draft released for review by Brad Moran.

INPUT AND REVIEW TABLE

Privacy Impact Assessment				
Name	**Position Title**	**Author**	**Contribute**	**Review**
Bill Boyte	Privacy Officer, Vancouver Island University			✓
Brad Moran	IT Business Architect, Vancouver Island University			✓
Moira Connor	Sr. Privacy Analyst, PrivacyWorks	✓		

[1] Complete a Privacy Impact Assessment - Province of British Columbia (gov.bc.ca)

DEFINITIONS

Acronym or Term	Description
Contact Information	Definition from FIPPA: *means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.*
FIPPA	*Freedom of Information and Protection of Privacy Act* *https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00*
Personal Information	means recorded information about an identifiable individual other than contact information and includes, but is not limited to: • Name, age, sex, weight, height • Home address and phone number • Race, ethnic origin, sexual orientation • Medical information • Health care history, including physical or mental disability • Number or symbol assigned to the individual • Income, purchases and spending habits • Blood type, DNA code, fingerprints • Marital or family status • Religion • Education • Financial information • Criminal information • Employment information • Personal views or opinions, except if they are about someone else • Personal Information - Province of British Columbia (gov.bc.ca)
PI	Personal Information
PIA	Privacy Impact Assessment
SOC 2	System and Organization Controls, Type 2
VIU	Vancouver Island University

TABLE OF CONTNETS

PART 1: GENERAL INFORMATION 1

1 INITIATIVE OVERVIEW 1
1.1 Description of In-Scope Applications 2
1.1.1 Microsoft Editor 2
1.1.2 Microsoft Forms 2
1.1.3 Microsoft OneNote 3
1.1.4 Microsoft Publisher 3
1.1.5 Microsoft Sway 4
1.1.6 Microsoft Whiteboard 5
2 PIA SCOPE 6
2.1 In Scope 6
2.2 Out of Scope 6
3 DATA OR INFORMATION ELEMENTS INCLUDED 6
3.1 Types of Information 6
3.2 Personal Information 9
4 REDUCING RISK OF UNINTENTIONAL PI COLLECTION OR DISCLOSURE 9
4.1 General 9
4.2 Editor 9
4.3 Forms 10
4.4 OneNote 10
4.5 Publisher 10
4.6 Sway 10
4.7 Whiteboard 10

PARTS: 2 – 8 – NOT APPLICABLE 10

PART 9: SIGNATURES 11

5 PRIVACY OFFICE 11
6 PROGRAM AREA SIGNATURES 12

PART 10 – APPENDICES 13

7 APPENDIX A: SUMMARY INFORMATION OF APPS 13
7.1 Microsoft Editor 13
7.2 Microsoft Forms 20
7.3 Microsoft OneNote 29
7.4 Microsoft Publisher 40
7.5 Microsoft Sway 49
7.6 Microsoft Whiteboard 63

PART 1: GENERAL INFORMATION

1 Initiative Overview

Vancouver Island University (VIU) is looking to integrate a variety of Microsoft products with their Microsoft 0365 subscription.

This privacy impact assessment (PIA) will focus on the following in-scope Microsoft products used for content creation, editing, and surveys.

- Microsoft Editor,
- Microsoft Forms,
- Microsoft OneNote,
- Microsoft Publisher,
- Microsoft Sway, and
- Microsoft Whiteboard.

This assessment is to be considered a genera**l,** or foundational**,** review of the in-scope products. In order to conduct specific privacy assessments of each product, VIU will need to:

- determine/document how VIU intends to use the products;
- define what user/customer data they will be collecting, using and disclosing;
- define who will have access to the products, and how that access will be managed; and
- define what configurations will be put in place to maximize privacy safeguards (including a “consent” box where applicable).

For purposes of this preliminary assessment, it has been assumed that VIU does not intend to collect Personal Information. Note that, depending on context, VIU end-user data such as name, phone number and email address may be considered business contact information, and thereby not covered by the *Freedom of Information and Protection of Privacy Act* (FIPPA).

This assessment uses the Province of BC’s Privacy Impact Assessment for Non-Ministry Public Bodies template (as of March 2023)[2]. Source information was derived from a diverse range of resources, including Microsoft documentation and publicly accessible web content.

[2] Complete a Privacy Impact Assessment - Province of British Columbia (gov.bc.ca)

1.1 Description of In-Scope Applications

1.1.1 Microsoft Editor

Microsoft Editor is an AI-powered writing assistant designed to help users improve their writing in various Microsoft products.

Editor offers the user suggestions on grammar, spelling, punctuation, style, and clarity to help the user communicate more effectively and professionally.

Editor is integrated into several Microsoft products, such as Word, Outlook, OneNote, and PowerPoint, as well as being available as a browser extension for Microsoft Edge and Google Chrome.

For additional information please refer to the Appendices Microsoft Editor.

1.1.2 Microsoft Forms

Microsoft Forms is a user-friendly, online application that allows users to create and share surveys, quizzes, polls, and other types of forms to collect data, feedback, or responses from various audiences. Forms is part of the Microsoft 365 suite of productivity tools.

Features and functionalities of Microsoft Forms include:

- **Form creation:** Microsoft Forms provides a drag-and-drop interface that enables users to easily add several types of questions (e.g., multiple choice, text, rating, date, and ranking) and customize the form's appearance, including themes, background colors, and images.
- **Branching logic:** Microsoft Forms supports branching logic, allowing users to create forms with different paths based on respondents' answers. This feature enables more dynamic and personalized form experiences for respondents.
- **Real-time response tracking:** Users can view form responses in real-time, as they are submitted. The responses can be analyzed directly within the application, with built-in data visualization tools such as charts and graphs.
- **Export data:** Microsoft Forms allows users to export response data to other formats, such as Excel or CSV files, for further analysis and reporting.
- **Sharing and collaboration:** Users can easily share forms with others, either within their organization or publicly, using a shareable link or QR code. Microsoft Forms also supports collaboration, enabling multiple users to co-author a form simultaneously.
- **Templates:** Microsoft Forms offers a range of pre-built templates for various scenarios, such as event registrations, customer feedback, or employee satisfaction surveys, to help users quickly create forms tailored to their needs.
- **Integration with other Microsoft applications**: Microsoft Forms can be integrated with other Microsoft 365 applications, such as Power Automate for automation, Power BI for advanced data analysis, and Microsoft Teams for seamless collaboration.

- **Security and compliance:** Microsoft Forms adheres to Microsoft's strict security and compliance standards, ensuring that the data collected is protected and stored securely. It also supports compliance with various data protection regulations, such as GDPR, HIPAA, and CCPA.

For additional information please refer to the Appendices Microsoft Forms.

1.1.3 Microsoft OneNote

Microsoft OneNote is a digital notebook application that offers a range of features designed to enhance productivity, organization, and collaboration.

OneNote users can:

- type notes or record audio at their laptop;
- sketch or write ideas on their tablet;
- add picture from their phone;
- find notes instantly;
- freely move notes around the page;
- organize those pages into sections;
- keep sections in one or more notebooks;
- switch devices and pick up right where they left off; and
- share their notebooks with others so they can all view and contribute at the same time.

OneNote allows users to create notes that can include texts, pictures, tables, and drawings. Unlike a word processor, OneNote features a virtually unbounded document window, in which users can click anywhere on the canvas to create a new text box at that location. OneNote saves data automatically as the user makes edits to their file.

OneNote supports real-time collaboration, allowing multiple users to work on the same notebook simultaneously. Users can share their notebooks with others, either by granting editing permissions or by sharing a read-only link. Changes made to the notebook are automatically synchronized across all devices, ensuring that everyone has access to the most up-to-date information.

OneNote notebooks can be stored on Microsoft's cloud storage platform, OneDrive. This enables users to access their notes from any device with an internet connection and ensures that their data is securely backed up.

For additional information please refer to the Appendices Microsoft OneNote.

1.1.4 Microsoft Publisher

Microsoft Publisher is a desktop publishing application that is part of the Microsoft Office Suite. It is primarily used to create professional-quality publications such as brochures, newsletters, flyers, postcards, greeting cards, calendars, and more. Key features and functionalities of Microsoft Publisher include:

- **Templates**: Microsoft Publisher comes with a variety of pre-designed templates that users can use to create their publications quickly. The templates cover a range of categories such as newsletters, brochures, flyers, postcards, business cards, and more.
- **Layout Options:** Microsoft Publisher provides users with a variety of layout options to choose from. These include different page sizes, page orientation (portrait or landscape), and margin settings.
- **Text Tools**: Users can add and customize text using a range of text tools. These tools include different font styles, sizes, colors, and effects such as bold, italic, underline, and more.
- **Graphics and Images**: Microsoft Publisher allows users to add and customize graphics and images to their publications. Users can insert pictures, clip art, shapes, and more. Additionally, they can edit the images using tools such as cropping, resizing, and rotating.
- **Printing and Sharing:** Once the publication is complete, users can print it directly from Publisher or save it as a PDF or XPS file. They can also share the publication via email, social media, or OneDrive.

For additional information please refer to the Appendices Microsoft Publisher

1.1.5 Microsoft Sway

Microsoft Sway is a cloud-based digital storytelling and presentation application developed by Microsoft, designed to help users create and share interactive reports, presentations, stories, newsletters, and other content quickly and easily.

Part of the Microsoft Office family, Sway is available as a standalone app, as well as through Office 365 subscriptions and Microsoft 365.

Key Features include:

- **User-friendly interface**: Sway offers a clean, intuitive interface that makes it simple for users to create visually appealing content without requiring design expertise.
- **Responsive design:** Sway automatically adapts the layout and design of the content to fit various devices, such as desktops, tablets, and smartphones, ensuring optimal user experience regardless of the viewing platform.
- **Multimedia integration**: Sway supports the seamless incorporation of a wide range of media types, including images, videos, audio, text, and embedded content from various sources like YouTube, Vimeo, and more.
- **Smart design suggestions:** The built-in Design Engine uses artificial intelligence to provide users with design suggestions that enhance their content. Users can modify the design theme, color scheme, and font styles or allow Sway to generate a design based on the content.
- **Collaboration:** Sway enables users to collaborate in real-time with colleagues or classmates, making it suitable for team projects, classroom assignments, and more.

Access to a Sway can be controlled by sharing a link or embedding it on a website or blog.

- **Accessibility:** Sway offers accessibility features such as keyboard navigation, screen reader support, and sharp contrast mode, ensuring that content is accessible to users with disabilities.
- **Cloud-based storage**: Sway projects are automatically saved and synchronized to the cloud, allowing users to access and edit their content from any device with internet access.
- **Privacy controls:** Users can set privacy settings for their Sway presentations, controlling who can view or edit the content. Settings range from private, where only the author has access, to public, where anyone with the link can view the Sway.

For additional information please refer to the Appendices Microsoft Sway.

1.1.6 Microsoft Whiteboard

Microsoft Whiteboard is a collaborative, digital canvas application designed to facilitate real-time communication, brainstorming, and teamwork among users. It allows participants to draw, sketch, write, and share ideas on a virtual whiteboard, making it ideal for both in-person and remote meetings or educational settings.

Key features of Microsoft Whiteboard include:

- **Infinite Canvas**: The application provides an extensive, zoomable canvas that allows users to add content without any space constraints. This ensures that all ideas, notes, and sketches can be captured in one place.
- **Real-time collaboration**: Multiple participants can simultaneously contribute to the whiteboard, making it easy to share ideas and collaborate effectively. Changes made by one user are visible to all participants in real-time, ensuring everyone stays on the same page.
- **Ink to Shape and Ink to Table**: Microsoft Whiteboard includes intelligent recognition tools that automatically convert hand-drawn shapes and tables into precise, uniform shapes and grids. This feature helps to keep the board organized and easy to understand.
- **Digital Inking:** Users can draw, write, or sketch with digital pens, highlighters, or markers, making the experience similar to using a physical whiteboard. The application supports an assortment of colors and pen thicknesses, enabling users to create visually engaging content.
- **Sticky Notes**: Participants can add sticky notes to the whiteboard to capture ideas or provide feedback without interfering with the main content. This feature is useful for organizing information, brainstorming, or voting on ideas.
- **Import and Embed**: Microsoft Whiteboard allows users to import images, documents, and other content directly onto the canvas, making it easy to reference external resources during a discussion or presentation.

- **Templates:** The application includes several pre-built templates designed for specific use cases, such as brainstorming, project planning, and problem-solving. These templates help users structure their work and get started quickly.
- **Accessibility:** The application includes accessibility features like a high-contrast mode and screen reader support, ensuring that it is usable by individuals with diverse needs.

For additional information please refer to the Appendices Microsoft Whiteboard.

2 PIA Scope

2.1 In Scope

This preliminary privacy impact assessment (PIA) is specific to the following Microsoft Content Creation Apps:

- Microsoft Editor,
- Microsoft Forms,
- Microsoft OneNote,
- Microsoft Publisher,
- Microsoft Sway, and
- Microsoft Whiteboard.

2.2 Out of Scope

This PIA assesses the in-scope content creation apps but does not assess specific use cases of those apps. Specific use cases are required to better understand how Vancouver Island University will use the app and what data they intend to collect, use, store, or disclose.

3 Data or Information Elements Included

3.1 Types of Information

A general summary of the types of information collected by each of the in-scope Microsoft applications is described in the table below.

Please note that the specific data collected and processed by these applications would vary depending on the user's settings and usage patterns. Additionally, Microsoft may update the data collection practices of these applications from time to time.

Application or Service	Types of Information Collected	Link to Detail Table
Microsoft Editor	• Textual data: Editor collects and processes textual data input by users, such as the text in a document or email. • Diagnostic data: Editor collects diagnostic data to improve the performance and	Microsoft Editor

Application or Service	Types of Information Collected	Link to Detail Table
	reliability of the application. This may include information about the user's device, operating system, and application usage.	
Microsoft Forms:	• Survey and quiz data: Forms collects and processes survey and quiz data input by users, such as answers to questions or ratings. • User information: Forms may collect user information such as name and email address to identify the user and associate their responses with their account. • Diagnostic data: Forms collects diagnostic data to improve the performance and reliability of the application. This may include information about the user's device, operating system, and application usage.	Microsoft Forms
Microsoft OneNote:	• Textual data: OneNote collects and processes textual data input by users, such as notes, lists, and emails. • Audio and video data: OneNote may collect, and process audio and video data recorded by users within the application. • User information: OneNote may collect user information such as name and email address to identify the user and associate their notes with their account. • Diagnostic data: OneNote collects diagnostic data to improve the performance and reliability of the application. This may include information about the user's device, operating system, and application usage.	Microsoft OneNote
Microsoft Publisher	• Document data: Publisher collects and processes document data input by users, such as text, graphics, and images. • User information: Publisher may collect user information such as name and email	Microsoft Publisher

Application or Service	Types of Information Collected	Link to Detail Table
	address to identify the user and associate their documents with their account. - Diagnostic data: Publisher collects diagnostic data to improve the performance and reliability of the application. This may include information about the user's device, operating system, and application usage.	
Microsoft Sway	- Presentation data: Sway collects and processes presentation data input by users, such as text, images, and videos. - User information: Sway may collect user information such as name and email address to identify the user and associate their presentations with their account. - Diagnostic data: Sway collects diagnostic data to improve the performance and reliability of the application. This may include information about the user's device, operating system, and application usage.	Microsoft Sway
Microsoft Whiteboard	- Whiteboard content: Whiteboard collects and processes the content created by users within the application, such as notes, images, and drawings. - User information: Whiteboard may collect user information such as name and email address to identify the user and associate their content with their account. - Diagnostic data: Whiteboard collects diagnostic data to improve the performance and reliability of the application. This may include information about the user's device, operating system, and application usage.	Microsoft Whiteboard

3.2 Personal Information

Depending on the context in which it is used, information that is specifically provided to contact a person at their place of business may not be considered personal information.

Upon identifying the specific VIU use-cases for each in-scope Microsoft application (Editor, Forms, OneNote, Publisher, Sway, and Whiteboard), VIU will need to assess whether each use-case intends to collect personal information or has a high likelihood of inadvertently collecting it.

The Microsoft apps included in this assessment that are most likely to collect personal information (beyond business contact information), include Forms, OneNote and Whiteboard.

- **Forms**: a form creator may unintentionally or intentionally create forms that request personal information from respondents (even sensitive PI such as gender or ethnicity).
- **OneNote:** users may include personal information within their notes, either intentionally or accidentally.
- **Whiteboard**: during brainstorming or collaborative sessions, users may unintentionally or intentionally share personal information, either by writing/including it on the canvas or by uploading files that contain personal information.

The Microsoft apps that are less likely to collect personal information include Editor, Publisher, and Sway.

- **Editor:** users may work on documents that contain personal information, but Editor does not inherently collect or store this data.
- **Publisher**: the primary purpose and design of Publisher make it less likely for personal information to be collected.
- Sway: users can include personal information within their Sway presentations, however, the application's design and primary purpose make it less likely for personal information to be collected.

4 Reducing Risk of Unintentional PI Collection or Disclosure

4.1 General

The actual VIU use of each of the Microsoft applications (Editor, Forms, OneNote, Publisher, Sway, and Whiteboard) would need to be assessed to determine the most appropriate means of reducing risk of unintentional PI collection or disclosure. However, the following privacy-related configurations (available to the VIU Microsoft administrator) could help minimize general privacy risks:

4.2 Editor

- Turn off the "Send Microsoft information about how I write" setting to prevent the app from collecting user input data.
- Configure privacy settings in Microsoft Endpoint Manager to prevent automatic data collection by the app.

- Disable data sharing with third-party services to prevent data from being shared with other organizations.

4.3 Forms

- Configure privacy settings in Microsoft Endpoint Manager to control data collection by the app.
- Turn off the "Allow sharing results" setting to prevent survey responses from being shared with others.
- Use access controls to limit who can view and edit forms and survey responses.

4.4 OneNote

- Disable the "Send usage data" setting to prevent OneNote from collecting usage data.
- Use access controls to limit who can view and edit notebooks.
- Enable encryption to protect data in transit and at rest.

4.5 Publisher

- Use access controls to limit who can view and edit documents.
- Turn off the "Allow Office to connect to online services" setting to prevent data from being shared with other organizations.
- Enable encryption to protect data in transit and at rest.

4.6 Sway

- Disable the "Allow Sway to send usage data to Microsoft" setting to prevent the app from collecting usage data.
- Use access controls to limit who can view and edit presentations.
- Enable encryption to protect data in transit and at rest.

4.7 Whiteboard

- Use access controls to limit who can view and edit whiteboards.
- Disable the "Allow Whiteboard to collect feedback and diagnostics" setting to prevent the app from collecting usage data.
- Enable encryption to protect data in transit and at rest.

PARTS: 2 – 8 – NOT APPLICABLE

For purposes of this foundational PIA, it has been assumed that VIU will not collect Personal Information, thereby completion of parts 2-8 of the PIA template are not required. Note that an addendum PIAs will be required if further VIU analysis determines use cases that may include Personal Information.

PART 9: SIGNATURES

5 PRIVACY OFFICE

Privacy Office Comments

Privacy Office Signatures

This PIA accurately documents in-scope Microsoft applications at the time of signing.

If there are any changes to the overall initiative, including if Personal Information will, or could, be collected, used, stored, or disclosed, the Vancouver Island University program area lead will engage with the privacy officer, and complete a PIA update.

Role	Name	Electronic signature	Date signed
Privacy Officer, Vancouver Island University	**Bill Boyte**		

6 PROGRAM AREA SIGNATURES

This PIA accurately documents in-scope Microsoft applications at the time of signing.

If there are any changes to the overall initiative, including if Personal Information will, our could, be collected, used, stored, or disclosed, the Vancouver Island University program area lead will engage with the privacy officer, and complete a PIA update.

Program Area Comments

Role	Name	Electronic signature	Date signed
IT Business Architect, Vancouver Island University	Brad Moran	[redacted]	May 10, 2023

s. 22(1)

PART 10 – APPENDICES

7 APPENDIX A: SUMMARY INFORMATION OF APPS

7.1 Microsoft Editor

The following table provides summary information on Microsoft Editor.

Category	Microsoft Editor
Description:	Microsoft Editor is an AI-powered writing assistant designed to help users improve their writing in various Microsoft products. Editor offers the user suggestions on grammar, spelling, punctuation, style, and clarity to help the user communicate more effectively and professionally. Editor is integrated into several Microsoft products, such as Word, Outlook, OneNote, and PowerPoint, as well as being available as a browser extension for Microsoft Edge and Google Chrome.
Platforms:	As part of Microsoft 365, and as integrated into Office apps.
Key Data Inputs:	Key data inputs to Microsoft Editor include: • **Text input**: The primary input for Editor is the text that users type or paste into a document, email, or any other supported platform. The Editor analyzes this text to identify errors, inconsistencies, and areas for improvement. • **Language model:** Editor uses an advanced language model trained on a large corpus of text from diverse sources. This model helps the Editor understand grammar, syntax, semantics, and context to provide relevant suggestions. • **User preferences**: Editor can be customized to suit users' preferences, such as setting the desired level of formality, inclusiveness, or using specific language rules. These preferences help tailor the suggestions to users' unique requirements. • **Contextual information**: Editor considers the context of the text to provide suggestions that are appropriate and meaningful. This includes understanding the surrounding

Category	Microsoft Editor
	text and the overall structure of the document, which helps in offering more precise and relevant suggestions. • **Multilingual support**: Editor has multilingual capabilities, allowing it to process and provide suggestions for texts written in different languages. Editor uses language-specific models to understand grammar, spelling, and stylistic rules of each supported language. • **User interaction data**: As users interact with Editor's suggestions, the system learns from users' choices, such as accepted or rejected recommendations, to improve the quality of its suggestions over time. • **Real-time collaboration data (if applicable**): When multiple users collaborate on a document, Editor uses real-time data to provide contextually relevant suggestions based on the changes made by different collaborators.
Collection of Diagnostic Data by Microsoft:	The diagnostic data collected by Microsoft Editor may include: • device and software configuration data; • performance data of the software; • error reports and crash data; • usage patterns and feature usage statistics; and • anonymized and aggregated text data to improve the language model. Optional diagnostic data for Office - Deploy Office | Microsoft Learn
Collection of Customer Data by Editor:	Editor does not collect or store the text users type or the documents they open while using the Editor service. However, Microsoft does collect customer data related to the usage of Editor to improve the service and overall user experience. According to Microsoft's privacy policy, the customer data that may be collected by Editor includes: • **Diagnostic data:** Microsoft collects diagnostic data about the features and performance of Editor, which helps them identify and fix issues, as well as improve the service. This data may include information about the device, operating system, software version, language settings, and other details related to the usage of Editor.

Category	**Microsoft Editor**
	• **Interaction data**: Microsoft may collect data about how users interact with Editor, such as the frequency of usage, which features are utilized, and user preferences. This information helps Microsoft understand how the service is used and allows them to refine and enhance the features based on user feedback and behavior patterns. • **Service improvement data**: Microsoft may use aggregated and anonymized data to analyze the effectiveness of Editor's AI algorithms, identify areas for improvement, and develop new features. This data does not include the text you type or the documents you open, and it is not linked to individual users or specific documents.
Data Collected or Processed in Editor:	According to Microsoft's privacy policy, the data that may be collected or processed by Editor includes: • Textual data: As you type, Editor analyzes the text in real-time to provide suggestions. While Editor does not store the text or documents, it temporarily processes and analyzes the text on Microsoft's servers. • Diagnostic data: Editor may collect diagnostic data about the features and performance of the service to identify and fix issues, as well as improve the service. This data may include information about the device, operating system, software version, language settings, and other details related to the usage of Editor. • Interaction data: Microsoft may collect data about how users interact with Editor, such as the frequency of usage, which features are utilized, and user preferences. This information helps Microsoft understand how the service is used and allows them to refine and enhance the features based on user feedback and behavior patterns. • Service improvement data: Microsoft may use aggregated and anonymized data to analyze the effectiveness of Editor's AI algorithms, identify areas for improvement, and develop new features. This data does not include the text you type or the documents you open, and it is not linked to individual users or specific documents.

Category	Microsoft Editor
	Note: Editor does not store or transmit the text or documents that a user types or opens while using the service. Instead, Editor temporarily processes and analyzes the text on Microsoft's servers to provide suggestions in real-time.
Personal Information Collected:	Editor does not directly collect personal information, but as an AI-based writing assistant, it may process text provided by the user, which could potentially contain personal information.
Customer Data Storage Location:	In Canada, Microsoft has two data center regions: • Canada Central: Located in Toronto, Ontario • Canada East: Located in Quebec City, Quebec Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Learn *Note that Microsoft Editor only temporarily processes the text data while providing suggestions to the user. It does not store the actual content of user documents or emails, except for anonymized and aggregated data to improve the language model.*
Built-In Integrations:	• Word • Outlook • Power Point • Microsoft Edge • Chrome (via extension)
Optional Integrations/Connections Requiring Configuration:	• Custom dictionaries • Style guide preferences • integration with third-party grammar and style checking tools, or document collaboration platforms like Google Docs.
Activity Logging - End-user controls:	No activity logging specific to Editor. Editor is integrated with other applications and the activity logging occurs within those applications.
User Activity Reports:	Editor does not provide User Activity Reports.

Category	Microsoft Editor
	VIU Administrators of a Microsoft 365 can access user activity reports for various Microsoft services, including Office applications like Word, Excel, and PowerPoint, where Microsoft Editor is integrated. Microsoft 365 admin center activity reports - Microsoft 365 admin | Microsoft Learn
Auditing:	No specific auditing of Editor as it is a feature within Word, Outlook, and other Microsoft Office apps.
Security Compliance:	Relevant Microsoft compliance: • ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). • SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Forms is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards:	Editor operates within other Microsoft applications like Word, Outlook, and PowerPoint, and adheres to the privacy and security settings configured for those applications, including data encryption and access controls.
Potential Privacy Risks:	There are limited privacy concerns with the use of Editor as it does not store text or documents. However, the analysis of user input for improving the AI algorithms could present a unique privacy risk in terms of potential exposure of sensitive textual data.

Category	Microsoft Editor
	• **Data collection**: As Microsoft Editor analyzes user input for grammar, spelling, and style suggestions, it may collect this data to improve the accuracy and effectiveness of its AI algorithms. The data collected may include sensitive or confidential information, such as personal details, proprietary information, or trade secrets that users might be working on. • **Data transmission**: When using cloud-based features of Microsoft Editor, user input data is transmitted to Microsoft's servers for processing. This transmission can pose a privacy risk if the data is intercepted, tampered with, or exposed during transit. • **Data storage and access**: Collected data may be stored on Microsoft's servers, potentially allowing access by Microsoft employees or third parties under specific circumstances. Even with strict security measures in place, there is always a risk of unauthorized access or data breaches, which can lead to the exposure of sensitive textual data. • **Data anonymization and aggregation**: Although Microsoft may anonymize and aggregate the collected data to minimize privacy risks, the possibility of re-identification remains. In some cases, sophisticated analysis techniques could potentially be used to link the anonymized data back to individual users or specific documents.
Privacy Risk Mitigations:	By Vancouver Island University Microsoft Administrator: • **Use secure transmission**: The organization can ensure that they use a secure connection to access the Editor service, such as a VPN or encrypted connection, to reduce the risk of interception or tampering of data in transit. • **Opt-out of diagnostic data collection**: The organization can choose to opt-out of the collection of diagnostic data by changing the privacy settings for their Microsoft account or the specific application. **By VIU – End Users:** • **Limit text input**: Users can limit the input text to only what is necessary to receive feedback from the Editor service, particularly for sensitive or confidential text.

Category	Microsoft Editor
	• **Use local processing**: Users can choose to use the locally installed version of Editor, which processes the text on the user's device and not on Microsoft's servers, to reduce the risk of data exposure during the continuous analysis of text. • **Use privacy settings**: Users can review and adjust their privacy settings in their Microsoft account or the specific application to better control the collection and use of their data.
Other Key Links:	• Free editorial software | Microsoft editor • Microsoft Editor checks grammar and more in documents, mail, and the web - Microsoft Support • Outlook advanced editing options - Microsoft Support • Editor settings in Outlook.com and Outlook on the web - Microsoft Support • Introducing Microsoft Editor – Bring out your best writer wherever you write - Microsoft Community Hub • Cloud Data Integrity at its Finest | Microsoft Trust Center • Microsoft Privacy Statement – Microsoft privacy

7.2 Microsoft Forms

Category	Microsoft Forms
Description:	Microsoft Forms is a user-friendly, online application that allows users to create and share surveys, quizzes, polls, and other types of forms to collect data, feedback, or responses from various audiences. Forms is part of the Microsoft 365 suite of productivity tools. Features and functionalities of Microsoft Forms include: • **Form creation:** Microsoft Forms provides a drag-and-drop interface that enables users to easily add several types of questions (e.g., multiple choice, text, rating, date, and ranking) and customize the form's appearance, including themes, background colors, and images. • **Branching logic:** Microsoft Forms supports branching logic, allowing users to create forms with different paths based on respondents' answers. This feature enables more dynamic and personalized form experiences for respondents. • **Real-time response tracking:** Users can view form responses in real-time, as they are submitted. The responses can be analyzed directly within the application, with built-in data visualization tools such as charts and graphs. • **Export data:** Microsoft Forms allows users to export response data to other formats, such as Excel or CSV files, for further analysis and reporting. • **Sharing and collaboration:** Users can easily share forms with others, either within their organization or publicly, using a shareable link or QR code. Microsoft Forms also supports collaboration, enabling multiple users to co-author a form simultaneously. • **Templates:** Microsoft Forms offers a range of pre-built templates for various scenarios, such as event registrations, customer feedback, or employee satisfaction surveys, to help users quickly create forms tailored to their needs. • **Integration with other Microsoft applications**: Microsoft Forms can be integrated with other Microsoft 365 applications, such as Power Automate

Category	Microsoft Forms
	for automation, Power BI for advanced data analysis, and Microsoft Teams for seamless collaboration. - **Security and compliance:** Microsoft Forms adheres to Microsoft's strict security and compliance standards, ensuring that the data collected is protected and stored securely. It also supports compliance with various data protection regulations, such as GDPR, HIPAA, and CCPA.
Platforms:	Web, iOS, and Android
Key Data Inputs:	- **Questions:** Users can input several types of questions into the survey or quiz, including multiple-choice questions, rating scales, open-ended questions, and more. The type of question used can affect the data collected and the analysis that can be performed on the results. - **Response options**: For multiple-choice questions or rating scales, users can input response options that the respondent can select from. This input is crucial to ensure that the data collected is relevant and useful for the intended purpose of the survey or quiz. - **Design and formatting**: Users can customize the design and formatting of the survey or quiz, including the layout, theme, and branding. This input can help make the survey or quiz more visually appealing and engaging for respondents. - **Distribution settings**: Users can choose various distribution settings, such as who can respond to the survey or quiz, how respondents can access the survey or quiz, and whether or not respondents can see previous responses. These inputs help control who can participate in the survey or quiz and how the data is collected. - **Analysis settings**: Users can also set various analysis settings, such as how responses are grouped, how data is displayed, and how to share the results. These inputs help users to analyze and understand the data collected and to share the results with others.
Collection of Diagnostic Data by Microsoft:	The following categories broadly describe the type of data collected across Microsoft applications: - **Device, connectivity, and configuration data:** This includes information about the device, operating system,

Category	Microsoft Forms
	browser, and installed applications or updates. Data about the device's network connection, like IP address and network provider, may also be collected. • **Product usage data**: This includes data about the features and functionalities used within the applications, how often they are used, and the duration of use. This data helps Microsoft understand user engagement and improve product features. • **Error reports and performance data**: Microsoft collects data about application crashes, hangs, and other errors, along with performance metrics like response times and resource usage. This data helps Microsoft identify and fix issues and improve application performance. • **Service usage data:** This includes data about the usage of connected cloud services, such as authentication, storage, and data synchronization. • **Support data:** When users contact Microsoft for support, additional data may be collected to help resolve the issue, such as error logs, troubleshooting data, and user feedback.
Collection of Customer Data by Forms:	Microsoft Forms collects customer data related to form responses and usage data. It depends on the specific questions and fields included in the form. The respondents provide this data when they fill out the form. Depending on the form, it **may** include: • **Personal information:** Names, email addresses, phone numbers, physical addresses, or other identifying details, depending on the questions asked in the form. • **Demographic data:** Age, gender, ethnicity, or other demographic information, if requested in the form. • **Preferences and opinions**: Data related to respondents' preferences, opinions, or choices based on the questions in the form, such as product preferences, satisfaction ratings, or feedback. • **User-generated content**: Any content created by respondents, such as text responses to open-ended questions or uploaded files, if the form allows for such submissions. In addition to the specific data collected through form responses, Microsoft Forms also collects usage data to

Category	Microsoft Forms
	improve the service and maintain its performance. This usage data may include: • Device and browser information: Details about the device, browser, and operating system used to access and submit the form. • IP address: The IP address of the respondent's device, which may be used for security, diagnostics, and geolocation purposes. • Usage patterns: Information about how users interact with the form, such as the time spent on the form, the order in which questions are answered, and any navigation or interaction events. *Note that Microsoft Forms is subject to Microsoft's data handling and privacy policies, which are designed to protect customer data and comply with applicable data protection regulations.* VIU should be aware of the data they collect through the application and act appropriately to protect sensitive information and ensure compliance with relevant privacy regulations.
Data Collected or Processed in Forms:	Microsoft Forms collects or processes: • **Survey responses**: Forms collects and stores the responses to the survey questions that respondents provide. This data is used to provide insight into the topics covered in the survey and to help the survey creator analyze the results. • **Metadata**: Forms also collects metadata related to the survey, such as the date and time the survey was created, the date and time the survey was last modified, and the number of responses received. This metadata is used to manage the survey and to provide information about how the survey is being used. • **Device and usage data**: Forms may collect device and usage data related to the respondent's use of the service, such as the type of device used, the browser version, the IP address, and other information related to the usage of the service. This data is used to help improve the service and to ensure that the service is functioning correctly.

Category	Microsoft Forms
	- **Diagnostic data**: Forms may collect diagnostic data related to the performance of the service, such as error messages, crash reports, and other information related to the performance of the service. This data is used to identify and fix issues with the service and to improve the overall user experience. *Note: Forms does not collect or process personal information, such as the names or email addresses of respondents, unless this information is explicitly requested in the survey questions. Forms is designed to prioritize privacy, and any data collected is used to improve the service and provide a better user experience.*
Personal Information Collected:	Microsoft Forms is designed to prioritize user privacy, and as such, it does not collect or process personal information unless explicitly requested in the survey questions. The personal information that may be collected by Forms includes: - **Name:** Survey creators may choose to request the respondent's name in the survey questions. - **Email address**: Survey creators may choose to request the respondent's email address in the survey questions, which can be used to send follow-up surveys or to contact the respondent directly. - **Other contact information**: Survey creators may choose to request other contact information, such as phone number or address, in the survey questions. *Note that if information collected is contact information (used to contact a person at their place of business), the information noted would not be considered Personal Information.*
Customer Data Storage Location:	In Canada, Microsoft has two data center regions: - Canada Central: Located in Toronto, Ontario - Canada East: Located in Quebec City, Quebec
Built-In Integrations:	- Excel, - OneDrive, - PowerPoint, - SharePoint,

Category	Microsoft Forms
	- Stream, - Sway, and - Teams.
Optional Integrations/Connections Requiring Configuration:	- Custom themes, - Third-party app integrations (using Power Automate)
Auditing:	Forms activities that are logged and available in the audit log include: - **Creation and modification of Forms**: When a user creates or modifies a Form, this activity is logged in the audit log, along with details such as the user who performed the action, the date and time of the action, and the type of action performed. - **Form sharing and collaboration:** When a user shares a Form or collaborates on a Form with other users, this activity is logged in the audit log, along with details such as the user who performed the action, the date and time of the action, and the users with whom the Form was shared or collaborated. - **Form response collection**: When a user collects responses to a Form, this activity is logged in the audit log, along with details such as the user who performed the action, the date and time of the action, and the number of responses received. - **Form deletion**: When a user deletes a Form, this activity is logged in the audit log, along with details such as the user who performed the action, the date and time of the action, and the type of action performed. - **Form data export**: When a user exports Form data, this activity is logged in the audit log, along with details such as the user who performed the action, the date and time of the action, and the type of action performed.
Security Compliance:	Relevant Microsoft compliance: - ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS).

Category	Microsoft Forms
	• SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Forms is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards in Forms:	• **Anonymous responses**: Forms allows users to choose whether or not to allow anonymous responses, which is a unique privacy safeguard not found in all Microsoft products and services. • **Data retention policies:** Forms includes specific privacy settings related to data retention, which allows users to control how long their data is stored and when it is deleted. This is a unique privacy safeguard that may not be present in other Microsoft applications. • **User collaboration controls**: Forms includes access controls that allow users to set permissions and restrictions on who can access and edit Forms and view survey responses. These controls are unique to Forms and are not present in all Microsoft products and services. • **Compliance certifications**: While compliance certifications are common across many Microsoft products and services, Forms has specific certifications that may not be present in other applications. For example, Forms is compliant with the US Children's Online Privacy Protection Act (COPPA), which is unique to Forms due to its use case in collecting data from children.
Potential Privacy Risks:	Since the primary purpose of Forms is to gather data from users, which could include personal information (PI) and other sensitive

Category	Microsoft Forms
	data, there is a high risk of non-compliance with FIPPA and privacy breaches. Specific areas of concern include: • **Collection of personal information:** When creating surveys, quizzes, or polls, form creators could request personal information such as names, email addresses, phone numbers, or physical addresses. This information may be necessary to identify respondents or for follow-up purposes, but it also introduces privacy concerns. • **Storage of sensitive data**: Data collected through Forms is stored in the cloud on Microsoft's servers. While Microsoft takes measures to secure this data, storing sensitive information in the cloud can increase the risk of unauthorized access or breaches. • **Sharing and collaboration**: Forms allows form creators to share forms with others, either within their organization or publicly. This sharing feature is useful for collaboration, but it can also expose sensitive information to unauthorized individuals if access permissions are not set up correctly. • **Exporting data:** Users can export data collected through Forms to other formats, such as Excel or CSV files. This exported data may include sensitive information, and if not protected, can be accessed by unauthorized parties. • **Integration with other applications**: Forms can be integrated with other applications, such as Power Automate or Power BI, for data analysis or automation purposes. When sensitive data is shared across multiple applications, the potential attack surface increases, making it more vulnerable to breaches. *Note that Microsoft Forms encrypts all of the data within the forms at rest and while in transit. The content in the forms is secure whether it is stored somewhere or it's going to another location electronically.*
Privacy Risk Mitigations:	Mitigations unique to Forms include: **<u>By the Vancouver Island University Microsoft Administrator</u>**: • **Implement access controls**: establish access controls to ensure that only authorized users can access and

Category	Microsoft Forms
	modify Forms data. This can help reduce the risk of unauthorized access or misuse of data. - **Conduct regular security assessments**: conduct regular security assessments of their Forms implementation to identify potential security vulnerabilities and ensure that data is being protected. - **Enable auditing and monitoring:** enable auditing and monitoring in Forms to track user activity and detect potential security incidents. - **Establish data retention policies**: establish data retention policies in Forms to specify how long data is retained and when it is deleted. This can help reduce the risk of unauthorized access to data. - **Educate users:** Train VIU users on best practices for creating and sharing Forms securely, and make sure they understand the importance of protecting sensitive information. **By the VIU End-User:** - **Create privacy-sensitive surveys:** create surveys that collect data in a privacy-sensitive manner. For example, they can limit the types of data they collect to only what is necessary and avoid collecting sensitive information. Ideally, create Forms that only collect anonymous responses. - **Limit access to Forms**: limit who has access to the Forms they create to reduce the risk of unauthorized access or misuse of data. - **Review and adjust privacy settings**: review and adjust privacy settings in Forms to better control the collection and use of their data. For example, they can choose whether or not to allow anonymous responses, set data retention policies, and determine how data is shared and accessed. - **Educate respondents**: educate survey respondents on how their data will be used and the steps being taken to protect their privacy. This can help build trust and reduce the risk of respondents providing inaccurate or incomplete data.
Key Links:	- Microsoft Forms (office.com) - Microsoft Forms | Surveys, Polls, and Quizzes

Category	Microsoft Forms
	• Introduction to Microsoft Forms - Microsoft Support • Set up Microsoft Forms - Microsoft Forms Admin | Microsoft Learn • Microsoft Forms help & learning • Microsoft Forms security: Using Microsoft Forms for sensitive data | The Jotform Blog

7.3 Microsoft OneNote

Category	Microsoft OneNote
Description:	Microsoft OneNote is a digital notebook application that offers a range of features designed to enhance productivity, organization, and collaboration. OneNote users can: • type notes or record audio at their laptop; • sketch or write ideas on their tablet; • add picture from their phone; • find notes instantly; • freely move notes around the page; • organize those pages into sections; • keep sections in one or more notebooks; • switch devices and pick up right where they left off; and • share their notebooks with others so they can all view and contribute at the same time. OneNote allows users to create notes that can include texts, pictures, tables, and drawings. Unlike a word processor, OneNote features a virtually unbounded document window, in which users can click anywhere on the canvas to create a new text box at that location. OneNote saves data automatically as the user makes edits to their file. OneNote supports real-time collaboration, allowing multiple users to work on the same notebook simultaneously. Users can share their notebooks with others, either by granting editing permissions or by sharing a read-only link. Changes made to the notebook are automatically synchronized across all

Category	Microsoft OneNote
	devices, ensuring that everyone has access to the most up-to-date information. OneNote notebooks can be stored on Microsoft's cloud storage platform, OneDrive. This enables users to access their notes from any device with an internet connection and ensures that their data is securely backed up.
Platforms:	Microsoft Office suite is available across multiple platforms, including Windows, macOS, Android, iOS, and the web.
Key Data Inputs:	OneNote allows users to create digital notebooks that can hold several types of content, such as text, images, audio recordings, video clips, and more. OneNote supports both drawing and handwriting inputs, allowing users to sketch, draw, or write using a stylus, touchscreen, or a mouse. The application has built-in handwriting recognition, which can convert handwritten notes into searchable text. Notebooks can be divided into sections and pages, making it easy to organize and navigate through the content.
Collection of Diagnostic Data by Microsoft:	Microsoft can collect Basic diagnostic data and Full diagnostic data. **Basic diagnostic data:** Basic diagnostic data is the minimum amount of information collected by Microsoft. This data is focused on understanding the device, its configuration, and whether the application is working properly. Basic diagnostic data may include: • **Device information:** Device type, hardware configuration, and operating system version. • **Application information**: OneNote version, installation details, and usage data (such as which features are used and how often). • **Error reports**: Details about application crashes or failures, which can help Microsoft identify and fix issues. • **Performance data:** Information about application responsiveness and resource usage.

Category	Microsoft OneNote
	• **Networking information**: Data about the device's connection to Microsoft services, such as OneDrive or SharePoint. **Full diagnostic data:** Full diagnostic data may include: • **Additional application usage data:** More granular information about how users interact with OneNote, such as the time spent on specific tasks or the use of certain features. • **Inking and typing data:** Information about user input, such as handwriting or typing, which can help improve handwriting recognition and other input-related features. *Note that this data is typically anonymized and separated from any personally identifiable information.* • **Content samples:** Microsoft may collect small samples of OneNote content, such as text, images, or audio, to help diagnose specific issues.
Collection of Customer Data by Microsoft:	The customer data collected by OneNote may include: • **Note content:** OneNote collects the content of notes created by users, including text, images, videos, and other multimedia content. • **User data:** OneNote collects user data such as usernames, email addresses, and profile pictures to personalize the application and enable collaboration features. • **Device and usage data**: OneNote may collect device and usage data, such as the type of device being used, the operating system and version, and how the user interacts with the application. This data is used to improve the application and troubleshoot issues. • **Metadata**: OneNote may collect metadata associated with notes, such as the creation and modification date, author name, and version history. This metadata is used to organize and search notes and enable collaboration features.
Data Collected or Processed in OneNote:	Microsoft collects and processes data such as: • **Note content:** OneNote collects and processes the content of notes created by users, including text, images, videos, and other multimedia content. This

Category	Microsoft OneNote
	data is stored in OneNote notebooks and is used to enable note-taking and collaboration features. • **User data**: OneNote collects and processes user data such as user-names, email addresses, and profile pictures to personalize the application and enable collaboration features. • **Device and usage data:** OneNote may collect and process device and usage data, such as the type of device being used, the operating system and version, and how the user interacts with the application. This data is used to improve the application and troubleshoot issues. • **Metadata:** OneNote collects and processes metadata associated with notes, such as the creation and modification date, author name, and version history. This metadata is used to organize and search notes and enable collaboration features. • **Feedback data:** OneNote may collect, and process feedback data submitted by users, such as feature requests or bug reports. This data is used to improve the application and troubleshoot issues.
Personal Information Collected or Processed in OneNote:	Information collected by Microsoft OneNote may include Personal Information: • **User-names**: OneNote may collect and process user-names to personalize the application and enable collaboration features. • **Email addresses**: OneNote may collect and process email addresses to enable collaboration features and send notifications to users. • **Profile pictures**: OneNote may collect and process profile pictures to personalize the application and enable collaboration features. • **Device and usage data**: OneNote may collect and process device and usage data, such as the type of device being used, the operating system and version, and how the user interacts with the application. While this data is not necessarily personal information on its own, it may become personal information if it is combined with other data to identify an individual.

Category	Microsoft OneNote
	Note that, depending on context, the user-names and email address may be considered business contact information, not personal information.
Customer Data Storage Location:	In Canada, Microsoft has two data center regions: • Canada Central: Located in Toronto, Ontario • Canada East: Located in Quebec City, Quebec
Built-In Integrations:	OneNote integrates seamlessly with other Microsoft Office applications, such as Word, Excel, PowerPoint, Outlook and Teams. *Note that these integrations may require configuration to enable features like embedding documents, sharing notes via email, or collaborating within Teams.*
Optional Integrations/Connections Requiring Configuration:	Optional OneDrive integrations include (but are not limited to): • Zapier: OneDrive can be connected to Zapier, a web-based automation tool that allows users to create custom workflows between different applications and services. • IFTTT: OneDrive can be connected to IFTTT (If This Then That), a web-based service that allows users to create custom actions based on triggers and conditions. • CloudHQ: OneDrive can be connected to CloudHQ, a cloud-based service that allows users to synchronize, back up, and migrate files across multiple cloud storage services. • CloudFuze: OneDrive can be connected to CloudFuze, a cloud migration and management tool that enables users to migrate files between different cloud storage services. • MultCloud: OneDrive can be connected to MultCloud, a cloud storage management tool that allows users to manage and transfer files between different cloud storage services. • FileCloud: OneDrive can be connected to FileCloud, a cloud-based file sharing and synchronization service that offers advanced security and data privacy features.

Category	Microsoft OneNote
	• Dropbox: OneDrive can be connected to Dropbox using third-party integration services such as CloudHQ, CloudFuze, or MultCloud, which allow users to transfer files between OneDrive and Dropbox. • Twitter: OneDrive can be connected to Twitter using third-party services such as IFTTT or Zapier, which allow users to automatically post tweets containing links to OneDrive files or to save tweets containing specific keywords to OneDrive. • Facebook: OneDrive can be connected to Facebook using the built-in Facebook integration, which allows users to share files and photos directly from OneDrive to Facebook. • LinkedIn: OneDrive can be connected to LinkedIn using the built-in LinkedIn integration, which allows users to share files and photos directly from OneDrive to LinkedIn.
Activity Logging - End-user controls:	OneDrive provides end-user activity logging controls that users can access and customize to better protect their privacy and security. Examples include: • **View and clear activity history**: OneDrive allows users to view their activity history, which includes a list of recent file and folder activity, such as uploads, downloads, edits, and deletions. Users can also clear their activity history to remove this data. • **Manage sharing links**: OneDrive allows users to manage sharing links for files and folders, including setting expiration dates, password protection, and access permissions. Users can also view a list of who has accessed shared files. • **Set access permissions**: OneDrive allows users to set access permissions for individual files and folders, including allowing or denying access to specific users or groups. • **Monitor sign-ins:** OneDrive allows users to monitor sign-ins to their account, including the time, location, and device used for each sign-in. • **Enable two-step verification**: OneDrive allows users to enable two-step verification, which adds an extra layer of security to their account by requiring a second form

Category	Microsoft OneNote
	of authentication, such as a code sent to their phone, when signing in.
User Activity Reports:	VIU Microsoft Administrators can monitor and track user activity. Reports that are available include: • File and folder activity report: This report provides information about file and folder activity, including uploads, downloads, edits, and deletions. • Sharing and collaboration activity report: This report provides information about sharing and collaboration activity, including shared links, access requests, and permissions changes. • Usage activity report: This report provides information about OneDrive usage, including the number of files and folders, storage usage, and active users. *Note: User activity reports can be accessed and customized by the administrators through the Microsoft 365 admin center.*
Auditing:	OneDrive provides an audit log that tracks and records user activity within an organization. The audit log captures various OneDrive activities and events, including: • **File and folder activity**: This includes uploads, downloads, modifications, and deletions of files and folders. • **Sharing and collaboration activity**: This includes sharing files and folders, granting or revoking access to files, and changes to sharing permissions. • **Sign-in activity**: This includes successful and failed sign-in attempts, as well as information about the device and location used to sign in. • **OneDrive usage**: This includes information about storage usage, the number of files and folders, and the number of active users. • **Administration activity:** This includes changes to OneDrive settings and configurations, as well as user and group management. *Note: The audit log can be accessed and customized by administrators through the Microsoft 365 admin center, and can be exported to various formats, such as CSV or XML, for further analysis.*

Category	Microsoft OneNote
Security Compliance:	Relevant Microsoft compliance: • ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). • SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Forms is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards:	Examples of OneNote privacy safeguards include: • **Encryption:** OneNote uses encryption to protect user data both in transit and at rest. This includes encrypting data as it is transmitted over the internet and encrypting data stored on Microsoft's servers. • **Access controls:** OneNote provides access controls to ensure that only authorized users can access and modify notes. This includes permissions-based access controls, two-factor authentication, and conditional access policies. • **Privacy settings:** OneNote provides users with privacy settings that allow them to control how their data is stored, accessed, and shared. This includes settings to control access to individual notes, control sharing and collaboration settings, and control settings related to data residency and compliance.
Potential Privacy Risks:	Privacy risks unique to OneNote include: • **Sensitive information stored in notes:** OneNote allows users to store a wide range of information in notes, including personal information, passwords, and

Category	Microsoft OneNote
	sensitive business information. This presents a privacy risk if these notes are not properly secured or if unauthorized users access them. - **Sharing and collaboration risks:** OneNote allows users to share and collaborate on notes with others, which can increase the risk of unauthorized access or disclosure of sensitive information. Organizations need to ensure that they have appropriate access controls in place to prevent unauthorized access and that users are aware of the risks associated with sharing and collaborating on notes. - **Data residency risks:** OneNote stores data in the cloud, which can present risks related to data residency and compliance with local data privacy laws and regulations. Organizations need to ensure that they understand where their data is stored, who has access to it, and how it is protected. - **Third-party integrations**: OneNote allows users to integrate with third-party applications and services, which can present privacy risks if these applications are not properly vetted or if they are accessed by unauthorized users. - **Use of AI and machine learning**: OneNote uses AI and machine learning to improve its functionality and provide personalized experiences for users. However, this presents a privacy risk if sensitive information is inadvertently analyzed or if user data is used for purposes that users did not intend or authorize.
Privacy Risk Mitigations:	<u>**By the Vancouver Island University Microsoft Administrator:**</u> - **Implement access controls**: implement access controls to ensure that only authorized users can access and modify notes. This includes permissions-based access controls, two-factor authentication, and conditional access policies. - **Provide privacy training**: provide privacy training to employees to educate them about the risks associated with using OneNote and how to use the application securely. This can help raise awareness about the risks of sharing and collaborating on notes, and how to properly secure sensitive information stored in OneNote.

Category	Microsoft OneNote
	• **Monitor user activity**: monitor user activity within OneNote to detect potential security incidents and ensure that user activity complies with organizational policies and regulations. This includes monitoring file and folder activity, sharing and collaboration activity, and sign-in activity. • **Perform regular security assessments**: perform regular security assessments to identify potential vulnerabilities within OneNote and implement appropriate security controls to mitigate these risks. This includes vulnerability scanning, penetration testing, and security audits. **By the VIU End-User:** • **Use strong passwords**: use strong passwords to protect their OneNote account. This includes using unique passwords for each account, using complex passwords that are difficult to guess, and changing passwords regularly. • **Avoid sharing sensitive information**: avoid storing and sharing sensitive information in OneNote, especially notes that are shared with others. Instead, sensitive information should be stored in more secure locations, such as encrypted files on a local device. • **Monitor sharing and collaboration settings**: monitor sharing and collaboration settings for notes and ensure that only authorized users have access to sensitive information. This includes setting appropriate access controls, monitoring shared links and access requests, and revoking access when necessary. • **Enable two-factor authentication**: enable two-factor authentication for their OneNote account, which adds an extra layer of security to the account and helps prevent unauthorized access.
Other Key Links:	• Microsoft Privacy Statement – Microsoft privacy • Deployment guide for OneNote - Deploy Office | Microsoft Learn • Frequently Asked Questions about OneNote in Office 2019 and Microsoft 365 - Microsoft Support

Category	Microsoft OneNote
	• OneNote help & learning (microsoft.com) • OneNote Essentials.pdf • OneNote for Team Collaboration.pdf • OneNote for Meetings.pdf • OneNote for Life Moments.pdf • OneNote-2016-Tips-Tricks.pdf • How Secure Is OneNote Online - Protect OneNote With Password (datarecovery.institute)

7.4 Microsoft Publisher

Category	Microsoft Publisher
Description:	Microsoft Publisher is a desktop publishing application that is part of the Microsoft Office Suite. It is primarily used to create professional-quality publications such as brochures, newsletters, flyers, postcards, greeting cards, calendars, and more. Key features and functionalities of Microsoft Publisher include: • **Templates**: Microsoft Publisher comes with a variety of pre-designed templates that users can use to create their publications quickly. The templates cover a range of categories such as newsletters, brochures, flyers, postcards, business cards, and more. • **Layout Options:** Microsoft Publisher provides users with a variety of layout options to choose from. These include different page sizes, page orientation (portrait or landscape), and margin settings. • **Text Tools**: Users can add and customize text using a range of text tools. These tools include different font styles, sizes, colors, and effects such as bold, italic, underline, and more. • **Graphics and Images**: Microsoft Publisher allows users to add and customize graphics and images to their publications. Users can insert pictures, clip art, shapes, and more. Additionally, they can edit the images using tools such as cropping, resizing, and rotating. • **Printing and Sharing:** Once the publication is complete, users can print it directly from Publisher or save it as a PDF or XPS file. They can also share the publication via email, social media, or OneDrive.
Platforms:	Microsoft Publisher is a desktop application that is available for Windows operating systems. It is not available for other operating systems such as macOS, Linux, or mobile platforms such as iOS or Android. However, users can still create and edit Publisher files on a Mac or other non-Windows operating system by using virtualization software or remote desktop access to a Windows machine that has Publisher installed.

Category	Microsoft Publisher
	Additionally, Publisher files can be exported to other file formats such as PDF or JPG that can be opened on other platforms.
Key Data Inputs:	Key data inputs to Microsoft Publisher depend on the type of publication that is being created. However, in general, common data inputs that can be used in Publisher include: • **Text:** Users can add and format text in Publisher. This can include headings, subheadings, body text, captions, and more. • **Images:** Users can add images to Publisher documents, such as photographs, clip art, logos, and other graphics. • **Design elements**: Publisher provides a range of design elements, such as backgrounds, borders, and frames, which can be added to publications. • **Layout:** Publisher allows users to choose and customize the layout of the publication, including page size, orientation, and margin settings. • **Template**: Publisher provides a variety of pre-designed templates that users can customize with their own content. • **Shape and Lines**: Users can insert and customize different shapes and lines, such as arrows and connectors, to create diagrams or flowcharts. • **Tables:** Users can add tables to their publications to present data in a structured format. • **QR Codes**: Publisher allows users to insert QR codes that can be scanned with a smartphone or tablet to access more information.
Collection of Diagnostic Data by Microsoft:	The specific diagnostic data that is collected by Microsoft when users use Publisher may include: • **Basic device and usage information**: This includes information such as the device type, operating system version, Publisher version, and language settings. • **Error reporting information**: This includes information about errors or crashes that occur while using Publisher, such as error messages, logs, and crash dumps. • **Performance and usage data**: This includes information about how users interact with Publisher, such as the frequency and duration of use, the features used, and the time taken to complete certain tasks.

Category	Microsoft Publisher
	• **Feature usage and customization data**: This includes information about how users customize and use specific Publisher features, such as fonts, colors, templates, and other design elements. • **Technical support information**: This includes information provided by users when they contact Microsoft technical support, such as the description of the issue, troubleshooting steps taken, and the outcome of the support interaction.
Collection of Customer Data by Publisher:	The types of customer data that Microsoft Publisher may collect includes: • **Account information**: If a user creates a Microsoft account to use Publisher, the application may collect and store the user's account information, such as name, email address, and password. • **Usage data:** Publisher may collect usage data to improve the application's functionality and performance. This may include information about how the application is used, such as the frequency and duration of use, the types of publications created, and the features and tools used within the application. • **Error reports:** Publisher may collect error reports to help diagnose and fix issues within the application. This may include information about errors encountered within the application, as well as information about the user's device and operating system. • **Customer feedback**: Publisher may collect customer feedback through surveys, polls, and other feedback mechanisms to improve the application's functionality and usability. This may include information about the user's satisfaction with the application, suggestions for new features, and feedback on existing features.
Data Collected and/or Processed by Publisher:	The types of data that Publisher may collect and/or process includes: • **File and document data:** Publisher may collect, and process data related to the files and documents that users create and edit within the application. This includes information about the file type, file size, and content of the document.

Category	Microsoft Publisher
	• **Usage data:** Publisher may collect and process usage data to improve the application's functionality and performance. This may include information about how the application is used, such as the frequency and duration of use, the types of publications created, and the features and tools used within the application. • **Device and system data**: Publisher may collect and process device and system data to help diagnose and troubleshoot issues with the application. This may include information about the user's device, operating system, and other software and hardware configurations. • **Error reports:** Publisher may collect and process error reports to help diagnose and fix issues within the application. This may include information about errors encountered within the application, as well as information about the user's device and operating system. • **Customer feedback**: Publisher may collect and process customer feedback through surveys, polls, and other feedback mechanisms to improve the application's functionality and usability. This may include information about the user's satisfaction with the application, suggestions for new features, and feedback on existing features.
Personal Information Collected in Publisher:	• **Account and user data**: Publisher may collect, and store account and user data related to the Enterprise subscription, such as user email addresses, account settings, and subscription usage data. This information is collected to help manage the Enterprise subscription and to provide personalized experiences for users. * • **Usage data**: Publisher may collect, and process usage data related to the Enterprise subscription, such as the frequency and duration of use, the types of publications created, and the features and tools used within the application. This information is collected to help improve the user experience and to provide personalized recommendations and suggestions. • **Enterprise-specific data**: Publisher may collect, and process data related to the Enterprise subscription, such as information about the organization's domain, usage patterns across the organization, and integration with

Category	Microsoft Publisher
	other Microsoft services. This information is collected to help manage the Enterprise subscription and to provide customized services and support. • **Customer feedback**: Publisher may collect and process customer feedback from Enterprise subscribers through surveys, polls, and other feedback mechanisms. This feedback is used to improve the application's functionality and to help prioritize new features and improvements for Enterprise subscribers. * ***Note:*** *Information that is typically used to contact a person at their place of business (such as name, phone number, and email address), is considered* ***contact*** *information, not personal information.*
Customer Data Storage Location:	Microsoft Publisher data is stored locally on the user's device unless the user chooses to store the data on a network or cloud storage service such as OneDrive or SharePoint.
Built-In Integrations:	Built-in Publisher integrations include: • **Microsoft Office**: Publisher is part of the Microsoft Office Suite, which includes other applications such as Word, Excel, and PowerPoint. This allows users to easily transfer data between applications and create integrated documents that combine text, images, and data from various sources. • **OneDrive and SharePoint:** Publisher is integrated with Microsoft's cloud storage and collaboration services, OneDrive and SharePoint. This allows users to store and share Publisher documents in the cloud, collaborate with others in real-time, and access their documents from any device with internet access. • **Microsoft Teams:** Publisher is integrated with Microsoft Teams, a collaboration platform that allows teams to chat, share files, and work together in real-time. Users can create and share Publisher documents within Teams and collaborate with others on the same document. • **Dynamics 365:** Publisher is integrated with Dynamics 365, Microsoft's customer relationship management (CRM) platform. This allows users to create and customize marketing materials, such as brochures and flyers, and

Category	Microsoft Publisher
	easily import data from Dynamics 365 to create personalized publications.
Optional Integrations/Connections Requiring Configuration:	There are optional integrations/connections that require configuration in Publisher, depending on the user's specific needs, including. These include, but are not limited to: • **Mail Merge**: Mail Merge is a feature in Publisher that allows users to merge a publication with a mailing list and print personalized copies of the publication. • **Data Sources**: Publisher allows users to import data from external data sources, such as Excel spreadsheets or Access databases, to create personalized publications. • **Print-to-PDF or XPS**: Publisher allows users to export their publications as PDF or XPS files. • **Printing Services:** Publisher allows users to send their publications to a professional printing service directly from the application. • **Social Media:** Publisher allows users to share their publications on social media platforms such as Facebook, Twitter, and LinkedIn.
Activity Logging - End-user controls:	Users can view and manage their data within Publisher by accessing their account settings and privacy options. For example, users can manage their account information, change their password, and adjust their privacy settings to control how their data is collected and used within the application. Additionally, users can submit feedback to Microsoft through the application's feedback mechanism, which may be used to improve the application's functionality and user experience.
User Activity Reports:	User activity reports may be available to the customer's administrator through Microsoft 365 admin center. Microsoft 365 admin center provides a range of management and monitoring tools for enterprise customers, including user activity reports for various Microsoft 365 applications, such as Publisher.
Auditing:	Examples of Publisher auditing capabilities that may be available to VIU's administrator include:

Category	Microsoft Publisher
	• **Document creation and editing:** Publisher may log when a user creates or edits a document within the application. This information may include the name of the document, the time and date it was created or edited, and the user who performed the action. • **Application usage**: Publisher may log how often the application is used, how long it is used for, and which features and tools are used most frequently. This information can provide insights into how the application is being used across an organization. • **Error reports**: Publisher may log error reports when a user encounters an error or issue within the application. These reports may include information about the error, the time and date it occurred, and the user who encountered the error. • **Customer feedback:** Publisher may log feedback from users through surveys, polls, and other feedback mechanisms. This feedback may be used to improve the application's functionality and user experience. *Note: the logging capabilities may depend on the version of Publisher and the settings configured by the administrator or user.*
Security Compliance:	Relevant Microsoft compliance: • ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). • SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Forms is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.

Category	Microsoft Publisher
Privacy Safeguards:	Publisher includes a range of privacy safeguards to help protect user data, including: • **Data encryption**: Publisher uses data encryption to protect user data while it is in transit between the application and Microsoft servers, as well as when it is stored on those servers. This helps to prevent unauthorized access to user data. • **Access controls**: Publisher includes access controls that allow users to control who has access to their data within the application. For example, users can control who they share their publications with, as well as who has access to their account settings and other personal information. • **Transparency and user control**: Publisher includes various features that provide transparency and user control over how their data is collected and used within the application. For example, users can manage their account settings and privacy options, as well as provide feedback and report issues with the application.
Potential Privacy Risks:	Examples of privacy risks that are unique to Publisher include: • **Sensitive information in publications**: One of the unique privacy risks associated with Publisher is the potential exposure of sensitive information in publications created by users. For example, a user may create a brochure or newsletter that includes personal information such as names, addresses, or phone numbers. If this publication is not properly secured or is shared with unauthorized users, it could result in the exposure of sensitive personal information. • **Risk of unauthorized access:** Publisher includes access controls to help protect user data, but there is still a risk of unauthorized access to publications and personal information. For example, if a user's account is compromised or their login information is stolen, unauthorized users could potentially gain access to their publications and personal data. • **Potential exposure of metadata**: Publisher includes metadata that can provide information about a publication, such as the author, creation date, and edit history. If this metadata is not effectively managed or

Category	Microsoft Publisher
	secured, it could potentially expose sensitive information about the publication and its creator. • **Data breaches and cyber attacks**: Like all software applications, Publisher is vulnerable to data breaches and cyber attacks that could result in the exposure or theft of user data. If a cyber criminal gains access to the application's servers or data storage, they could potentially steal sensitive user information or use it for malicious purposes.
Privacy Risk Mitigations:	Risk mitigations to address the unique privacy risks associated with Microsoft Publisher can include those done by administrators and those done by end-users. By Vancouver Island University Microsoft Administrator: • **Train users on privacy best practices**: Administrators can provide training and resources to users on privacy best practices, such as properly securing publications, limiting access to sensitive information, and following data security protocols. • **Implement access controls**: Administrators can implement access controls within Publisher to limit who has access to sensitive information and publications. This can include creating user groups with specific permissions, restricting access to certain features, and requiring multi-factor authentication. • **Monitor for unauthorized access**: Administrators can monitor Publisher usage and audit logs for signs of unauthorized access or suspicious activity. This can include reviewing access logs, monitoring for unusual login activity, and investigating any reported security incidents. By the VIU End-User: • **Secure publications:** End-users can take steps to secure their publications by using strong passwords, limiting access to sensitive information, and properly configuring sharing and collaboration settings. • **Password protect documents:** By adding a password to a publication, users can ensure that only authorized individuals with the password can access the content.

Category	Microsoft Publisher
	• **Manage metadata:** End-users can manage the metadata included in their publications to limit the exposure of sensitive information. This can include removing metadata that is not necessary, limiting the visibility of metadata, and properly configuring metadata settings.
Other Key Links:	Desktop Publishing Software | Download MS Publisher (microsoft.com) Publisher help & learning (microsoft.com) Basic tasks in Publisher - Microsoft Support Diagnostic data in Microsoft 365 - Microsoft Support

7.5 Microsoft Sway

Category	Microsoft Sway
Description:	Microsoft Sway is a cloud-based digital storytelling and presentation application developed by Microsoft, designed to help users create and share interactive reports, presentations, stories, newsletters, and other content quickly and easily. Part of the Microsoft Office family, Sway is available as a standalone app, as well as through Office 365 subscriptions and Microsoft 365. Key Features include: • **User-friendly interface**: Sway offers a clean, intuitive interface that makes it simple for users to create visually appealing content without requiring design expertise. • **Responsive design:** Sway automatically adapts the layout and design of the content to fit various devices, such as desktops, tablets, and smartphones, ensuring optimal user experience regardless of the viewing platform. • **Multimedia integration**: Sway supports the seamless incorporation of a wide range of media types, including images, videos, audio, text, and embedded content from various sources like YouTube, Vimeo, and more.

Category	Microsoft Sway
	• **Smart design suggestions:** The built-in Design Engine uses artificial intelligence to provide users with design suggestions that enhance their content. Users can modify the design theme, color scheme, and font styles or allow Sway to generate a design based on the content. • **Collaboration:** Sway enables users to collaborate in real-time with colleagues or classmates, making it suitable for team projects, classroom assignments, and more. Access to a Sway can be controlled by sharing a link or embedding it on a website or blog. • **Accessibility:** Sway offers accessibility features such as keyboard navigation, screen reader support, and sharp contrast mode, ensuring that content is accessible to users with disabilities. • **Cloud-based storage**: Sway projects are automatically saved and synchronized to the cloud, allowing users to access and edit their content from any device with internet access. • **Privacy controls:** Users can set privacy settings for their Sway presentations, controlling who can view or edit the content. Settings range from private, where only the author has access, to public, where anyone with the link can view the Sway.
Platforms:	• Web browser • Windows app for Windows devices • iOS app • While there is not a dedicated app for Android devices, users can access and edit their Sways through the web browser on their Android smartphones or tablets by visiting sway.office.com.
Key Data Inputs:	Key Sway data inputs include: • **Text:** Users can add text boxes, headings, subheadings, and paragraphs to their Sway to provide context and information. Text formatting options like bold, italics, underline, and bullet points are available to enhance readability and organization. • **Images:** Sway supports the integration of images in various formats (e.g., JPEG, PNG, GIF). Users can upload images from their devices, use images stored in

Category	Microsoft Sway
	OneDrive or other cloud storage services, or search for images through Bing's built-in image search, which prioritizes Creative Commons licensed images. • **Videos:** Users can embed videos from various sources, such as YouTube, Vimeo, or their own uploaded videos. These videos can be added directly by providing a URL or by searching within the Sway interface. • **Audio:** Sway enables users to add audio files or embed audio from platforms like SoundCloud or Spotify. Users can upload their own audio files or use the integrated search to find and include audio from external sources. • **Embed codes**: Sway supports the embedding of content from a wide range of web-based sources using embed codes, such as maps from Google Maps or Bing Maps, social media posts from Twitter or Facebook, and interactive content from other websites. • **Documents:** Users can incorporate content from documents created in other Microsoft Office applications, like Word, Excel, or PowerPoint. These can be uploaded directly or linked from OneDrive, SharePoint, or other cloud storage services. • **Charts and graphs**: Sway allows users to create and include charts, graphs, or other data visualizations to enhance their presentations and make data more accessible and understandable. • **External links**: Users can add hyperlinks to external websites or resources, providing additional context or directing viewers to further information.
Collection of Diagnostic Data by Microsoft:	The diagnostic data collected can be broadly categorized into two types: **Basic diagnostic data:** • **Device information**: Sway may collect information about the user's device, such as the device type, operating system version, and system configuration. This helps Sway understand the types of devices that are using the application and ensure that the application is optimized for those devices. • **Usage data:** Sway may collect usage data, such as how often the application is used, which features are used most frequently, and how long users spend on each feature. This helps Sway understand how users are using

Category	Microsoft Sway
	the application and identify areas for improvement or optimization. • **Performance data:** Sway may collect performance data, such as how long it takes for the application to load, how quickly pages and presentations are rendered, and how much memory and CPU the application uses. This helps Sway identify performance bottlenecks and optimize the application for faster performance. • **Error data**: Sway may collect error data, such as information about crashes, bugs, and other errors that occur within the application. This helps Sway identify and fix bugs and errors to improve the stability and reliability of the application. **<u>Optional diagnostic data:</u>** In addition to the basic diagnostic data, Sway also allows users to opt-in to additional diagnostic data collection. This optional diagnostic data may include: • **Feedback data:** Sway may collect feedback data, such as user feedback and suggestions for improving the application. This helps Sway understand user needs and prioritize improvements to the application. • **Account information**: Sway may collect account information, such as the user's name and email address, to help personalize the user experience and provide better support. • **App usage data:** Sway may collect app usage data, such as which features and functions are used most frequently, to help improve the user experience and optimize the application. • **Link tracking data**: Sway may track links clicked within presentations to help understand how users engage with content and optimize the user experience.
Collection of Customer Data by Sway:	Sway collects the following customer data: • **Account information**: Sway collects account information when users sign up for the application, such as the user's name, email address, and password. This information is used to identify the user and personalize their experience within the application. • **Usage data**: Sway collects usage data, such as how often the application is used, which features are used

Category	Microsoft Sway
	most frequently, and how long users spend on each feature. This information is used to optimize the application and improve the user experience. • **Content data:** Sway collects content data, such as the text, images, videos, and other media that users upload or create within the application. This information is used to display and share content within the application. • **Feedback data:** Sway collects feedback data, such as user feedback and suggestions for improving the application. This information is used to prioritize improvements to the application and provide better support to users.
Data Collected and/or Processed by Sway:	The types of data collected or processed in Sway include: • **Account information**: When users sign into Sway using their Microsoft account or Office 365 subscription, basic account information such as name, email address, and profile picture is collected to identify and authenticate the user. • **Content**: Microsoft Sway collects and processes the content users create, edit, and share within the app. This includes text, images, videos, audio, embedded content, documents, charts, and graphs that users add to their Sway presentations. • **Usage data:** Sway collects information about how users interact with the application, including the features used, frequency and duration of use, and any errors or issues encountered. This data helps Microsoft understand how Sway is being used and identify areas for improvement. • **Device and performance data**: Microsoft collects data about the devices used to access Sway, such as device type, operating system, browser, and other configuration settings. This data is used to optimize the performance of Sway across different devices and platforms. • **Collaboration data**: When users collaborate on a Sway project with others, data about the sharing and collaboration activities, such as invitations sent, permissions granted, and edits made by collaborators, may be collected.

Category	Microsoft Sway
	• **Feedback:** Microsoft may collect user-generated feedback, such as comments, suggestions, or problem reports, to improve Sway and address user concerns. • **Location data**: Sway may collect location data from users to provide localized experiences within the application. • **Diagnostic data**: Sway may collect diagnostic data to help improve the application and provide a better user experience. This may include device information, usage data, performance data, error data, and feedback data. • **Advertising data**: Sway may use advertising data, such as user preferences and behavior, to provide more relevant advertisements within the application.
Personal Information Collected:	The personal information collected in Sway includes: • **Account information**: When users sign into Sway using their Microsoft account or Office 365 subscription, basic account information such as name, email address, and profile picture is collected to identify and authenticate the user. This information also enables personalization of the Sway experience. • **Content:** The content created, edited, or shared within Sway may contain personal information added by users, such as names, email addresses, or other personally identifiable information in the text, images, or embedded content. • **Communication data**: When users share a Sway presentation with others or collaborate on a project, personal information like email addresses or names of collaborators may be collected. This information is necessary to enable sharing, collaboration, and permission management within Sway. • **Feedback:** If users provide feedback about Sway through comments, suggestions, or problem reports, any personal information they choose to include in their feedback may be collected. • **Location data**: Sway may collect location data from users to provide localized experiences within the application. • **Diagnostic data:** Sway may collect diagnostic data to help improve the application and provide a better user experience. This diagnostic data may include device

Category	Microsoft Sway
	information, usage data, performance data, error data, and feedback data. - **Advertising data:** Sway may use user preferences and behavior, to provide more relevant advertisements within the application.
Customer Data Storage Location:	When a user creates, edits, or shares a Sway, the content is automatically saved and synchronized to Microsoft's cloud servers, making it accessible from any device with an internet connection. This also ensures that the data is backed up and protected in the event of a device failure or loss. In Canada, Microsoft has two data center regions: - Canada Central: Located in Toronto, Ontario - Canada East: Located in Quebec City, Quebec
Built-In Integrations:	Sway's integrations include: - **Microsoft Office Suite:** Sway is designed to work seamlessly with other Microsoft Office applications like Word, Excel, and PowerPoint. Users can import content from these applications or link to documents stored in OneDrive, SharePoint, or other cloud storage services. - **OneDrive:** Sway integrates with OneDrive, Microsoft's cloud storage service, enabling users to access, upload, and embed files stored in their OneDrive directly within their Sway presentations. - **Bing Image Search**: Sway includes built-in Bing Image Search functionality, allowing users to search for and incorporate Creative Commons licensed images directly into their presentations. - **YouTube and Vimeo**: Sway supports embedding videos from popular video-sharing platforms like YouTube and Vimeo. Users can add videos by providing the URL or using the integrated search functionality. - **Social media platforms**: Sway allows users to embed content from social media platforms such as Twitter and Facebook, providing a dynamic and interactive element to presentations. - **Maps:** Sway supports embedding maps from mapping services like Google Maps or Bing Maps, allowing users to incorporate geographical context into their presentations.

Category	Microsoft Sway
	• **SoundCloud and Spotify**: Sway integrates with popular audio platforms like SoundCloud and Spotify, enabling users to add audio content to their presentations using the integrated search functionality or by providing a URL. • **Web-based content**: Users can embed content from various web-based sources using embed codes, such as interactive quizzes, polls, or other web-based applications.
Optional Integrations/Connections Requiring Configuration:	Connections and content types that may require additional steps or workarounds to incorporate into Sway include: • **Embed codes**: For web-based content that does not have a built-in integration in Sway, you can use embed codes to incorporate the content into your presentation. You will need to obtain the embed code from the source website and paste it into Sway's "Embed" content card. • **Custom fonts**: Sway does not currently support the direct import of custom fonts. However, you can create images with your custom font using graphic design software and then insert these images into your Sway presentation to maintain your desired typography. • **Third-party cloud storage services**: Sway integrates seamlessly with OneDrive but does not have built-in support for other cloud storage services like Google Drive or Dropbox. To incorporate content from these services, you can either download the files to your device and then upload them to Sway or, in some cases, obtain a shareable link or embed code and add it to Sway using the "Embed" content card. • **Other media platforms**: While Sway has built-in integrations for popular platforms like YouTube, Vimeo, SoundCloud, and Spotify, you may need to obtain embed codes or shareable links for media hosted on other platforms and then incorporate them using the "Embed" content card.
Activity Logging - End-user controls:	Microsoft Sway offers logging controls to end-users to manage the logging of their activities within the application. • **Privacy settings**: Sway provides users with privacy settings to control the collection and use of their data.

Category	Microsoft Sway
	Within the privacy settings, users can choose to turn off data collection and personalized advertising, as well as control the sharing of their data with third-party services. - **Opt-out of diagnostic data collection**: Sway allows users to opt-out of some or all diagnostic data collection within the privacy settings. This includes the ability to disable diagnostic data collection for error reporting and to prevent the collection of usage data and other diagnostic information. - **Opt-out of personalized advertising**: Sway allows users to opt-out of personalized advertising within the privacy settings. This prevents Sway from using user data to provide more relevant ads within the application. - **Clear browsing history**: Sway allows users to clear their browsing history within the application. This removes any history of pages visited within the application and may prevent some logging of user activities.
User Activity Reports:	Microsoft Sway provides user activity reports to help administrators track and monitor user activity within the application. - **Activity logs**: Sway provides activity logs that track user activity within the application. This includes details such as when a user signed in or out, which features were accessed, and which files were opened. - **Sharing activity**: Sway tracks sharing activity within the application, including which files were shared, who they were shared with, and the level of access granted to the shared files. - **Editing activity**: Sway tracks editing activity within the application, including which files were edited, who edited them, and the changes that were made. - **Content views**: Sway provides content view reports that show which files were viewed by users within the application. - **Usage reports:** Sway provides usage reports that show how often the application is used, which features are used most frequently, and how long users spend on each feature.

Category	Microsoft Sway
Auditing:	Microsoft Sway logs several types of user activities within the application to help administrators track and monitor user behavior. • **Sign-in and sign-out activity:** Sway logs when users sign in and sign out of the application. This includes the date and time of the sign-in and sign-out activity, as well as the user's account information. • **File and folder activities:** Sway logs when files and folders are created, opened, edited, deleted, and restored within the application. This includes details such as the name and location of the file or folder, the user who performed the activity, and the date and time of the activity. • **Sharing activities:** Sway logs when files and folders are shared within the application. This includes details such as the name and location of the file or folder, the user who shared the file or folder, and the user or group with which it was shared. • **Publishing activities:** Sway logs when presentations are published or unpublished within the application. This includes details such as the name of the presentation, the user who published or unpublished it, and the date and time of the activity. • **Viewing activities:** Sway logs when files and presentations are viewed within the application. This includes details such as the name and location of the file or presentation, the user who viewed it, and the date and time of the activity. • **Usage activities:** Sway logs usage activities within the application, such as which features are used most frequently, how long users spend on each feature, and how often the application is used.
Security Compliance:	Relevant Microsoft compliance: • ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). • SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance,

Category	Microsoft Sway
	demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Forms is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards in Sway:	Microsoft Sway provides several privacy safeguards to protect user data and ensure that it is used only for its intended purposes, including, but not limited to: • **Data encryption**: Sway uses industry-standard encryption to protect user data when it is transmitted over the internet. This helps prevent unauthorized access to user data during transmission. • **User access controls**: Sway provides user access controls that allow administrators to control which users have access to specific files and presentations within the application. This helps prevent unauthorized access to sensitive data. • **Privacy settings**: Sway provides privacy settings that allow users to control the collection and use of their data. Within the privacy settings, users can choose to turn off data collection and personalized advertising, as well as control the sharing of their data with third-party services. • **Data retention controls**: Sway allows administrators to set data retention policies that control how long user data is retained within the application. This helps ensure that user data is not stored for longer than necessary. • **Compliance certifications**: Sway is certified to comply with several industry-specific compliance standards, such as HIPAA, FERPA, and ISO 27001. This helps ensure that user data is stored and processed in accordance with applicable privacy laws and regulations. • **Privacy notice**: Sway provides a privacy notice that outlines how user data is collected, used, and shared

Category	Microsoft Sway
	within the application. The privacy notice provides transparency into how user data is handled within the application.
Potential Privacy Risks:	Potential privacy risks associated with Sway include, but are not limited to: • **Unintentional data sharing**: ○ Users can share their Sway presentations with others, both within and outside their organization. Sharing a presentation may expose sensitive information to unintended recipients if users do not effectively manage access permissions and sharing settings. ○ Sway integrates with various third-party services, such as YouTube, Vimeo, and social media platforms. When users incorporate content from these sources, they may inadvertently share sensitive information or expose their data to potential privacy risks associated with those third-party services. ○ The privacy of a Sway presentation is highly dependent on user behavior. Users may unintentionally share personal information, either by including it in their presentations or by sharing the presentation • **Unauthorized access**: Sway accounts may be compromised through phishing or other security breaches, which could lead to unauthorized access to user data within the application. • **Data leakage**: Sway may leak data through third-party integrations or by exporting presentations to other formats. This can result in the exposure of sensitive data and potentially violate data protection laws. • **Malware and viruses**: Users may inadvertently upload malware or viruses within Sway, which can compromise the security and privacy of user data within the application. • **Tracking and profiling**: Sway may track and profile user behavior within the application, which can potentially be used for advertising or other purposes.

Category	Microsoft Sway
	Note: These privacy risks are not unique to Sway and are common to many online applications.
Privacy Risk Mitigations:	Risk mitigations that can address potential privacy risks associated with Microsoft Sway include, but are not limited to, those noted below. <u>**By the Vancouver Island University Microsoft Administrator**</u>: • **User access controls:** implement user access controls to ensure that only authorized users have access to sensitive data within Sway. This can include limiting access to certain files and presentations or implementing role-based access controls. • **Data retention policies**: implement data retention policies that control how long user data is stored within Sway. This can help ensure that data is not stored for longer than necessary and reduce the risk of data breaches. • **Third-party integrations**: vet third-party integrations with Sway to ensure that they meet their privacy and security requirements. This can include reviewing privacy policies and security controls before enabling any integrations. • **Security monitoring:** implement security monitoring to detect and respond to security breaches within Sway. This can include implementing intrusion detection and prevention systems and monitoring access logs for suspicious activity. • **Malware protection**: keep software up to date, including antivirus software. • **User training:** provide user training to help end users understand the potential privacy risks associated with Sway and how to protect their data within the application. <u>**By the VIU End-User:**</u> • **Privacy settings**: review and manage their privacy settings in their Microsoft accounts and devices to control the data collected by Microsoft across their products and services, including Sway. • **Sharing permissions**: When sharing Sway presentations, users should be cautious about granting

Category	Microsoft Sway
	access to only intended recipients. Double-check sharing settings and permissions to avoid accidental exposure of sensitive information. • **Secure content creation**: While creating Sway presentations, users should avoid including sensitive or confidential information that could put their privacy or the organization's data at risk. If necessary, use alternative methods to present sensitive information, such as password-protected documents or secure communication channels. • **Third-party integrations**: Be cautious when incorporating content from third-party sources, as it may expose data to potential privacy risks associated with those services. Users should ensure they understand the privacy policies and data handling practices of these third-party services before embedding content in their Sway presentations. • **Password protection**: If a Sway presentation contains sensitive information, users can add password protection to restrict access. By setting a strong, unique password, users can mitigate the risk of unauthorized access to their presentations. *Note: These risk mitigations are not exhaustive and that additional measures may be necessary depending on the specific privacy risks associated with a given organization or user.*
Key Links:	• Microsoft Privacy Statement – Microsoft privacy • Getting Started with Sway - Microsoft Support • Create in Sway - Microsoft Support • Frequently asked questions about Sway – Admin Help - Microsoft Support • Administrator settings for Sway - Microsoft Support • Embed content in your Sway - Microsoft Support

7.6 Microsoft Whiteboard

Category	Microsoft Whiteboard
Description:	Microsoft Whiteboard is a collaborative, digital canvas application designed to facilitate real-time communication, brainstorming, and teamwork among users. It allows participants to draw, sketch, write, and share ideas on a virtual whiteboard, making it ideal for both in-person and remote meetings or educational settings. Microsoft Whiteboard is available as a standalone app on Windows, iOS, and web platforms and can also be accessed within Microsoft Teams. Key features of Microsoft Whiteboard include: • **Infinite Canvas**: The application provides an extensive, zoomable canvas that allows users to add content without any space constraints. This ensures that all ideas, notes, and sketches can be captured in one place. • **Real-time collaboration**: Multiple participants can simultaneously contribute to the whiteboard, making it easy to share ideas and collaborate effectively. Changes made by one user are visible to all participants in real-time, ensuring everyone stays on the same page. • **Ink to Shape and Ink to Table**: Microsoft Whiteboard includes intelligent recognition tools that automatically convert hand-drawn shapes and tables into precise, uniform shapes and grids. This feature helps to keep the board organized and easy to understand. • **Digital Inking:** Users can draw, write, or sketch with digital pens, highlighters, or markers, making the experience similar to using a physical whiteboard. The application supports an assortment of colors and pen thicknesses, enabling users to create visually engaging content. • **Sticky Notes**: Participants can add sticky notes to the whiteboard to capture ideas or provide feedback without interfering with the main content. This feature is useful for organizing information, brainstorming, or voting on ideas. • **Import and Embed**: Microsoft Whiteboard allows users to import images, documents, and other content directly

Category	Microsoft Whiteboard
	onto the canvas, making it easy to reference external resources during a discussion or presentation. • **Templates:** The application includes several pre-built templates designed for specific use cases, such as brainstorming, project planning, and problem-solving. These templates help users structure their work and get started quickly. • **Accessibility:** The application includes accessibility features like a high-contrast mode and screen reader support, ensuring that it is usable by individuals with diverse needs.
Platforms:	Microsoft Whiteboard is available as a standalone app on Windows, iOS, and web platforms and can also be accessed within Microsoft Teams.
Key Data Inputs:	• Freehand drawing and writing • Text • Sticky Notes • Images • Documents • Templates • Shapes and Lines • Ink to Shape and Ink to Table
Collection of Diagnostic Data by Whiteboard:	Microsoft collects diagnostic data from its products and services, including Microsoft Whiteboard, to improve performance, identify issues, and enhance user experience. The diagnostic data collected by Microsoft can be broadly categorized into two levels: Basic and Full. • **Basic Diagnostic Data:** This data is essential for maintaining the reliability and security of the software. Basic diagnostic data includes: ○ **Device information**: Device model, manufacturer, hardware configuration, and identifiers. ○ **Application data**: Information about installed applications, version numbers, and usage data. ○ **Performance data**: Metrics about the performance of the device, operating system, and applications.

Category	Microsoft Whiteboard
	○ **Network information**: Data about the network connections, like IP addresses, network type, and carrier. ○ **Error reporting**: Details about errors or issues encountered while using the software, such as crash reports and details of the problem. • **Full Diagnostic Data:** Full diagnostic data includes everything in the Basic level, as well as additional information that provides more context about the usage patterns and issues encountered. This data helps Microsoft better understand and resolve problems, as well as optimize user experience. Full diagnostic data may include: ○ **Inking and typing data**: Information about how users interact with input devices, like keyboards, touchscreens, and digital pens. ○ **Detailed usage data**: Information about how users interact with applications and features, including button clicks, menu selections, and feature usage patterns. ○ **Enhanced error reporting**: More detailed error reports that may include memory snapshots or other diagnostic information to help Microsoft identify and resolve issues. ○ **Customization data:** Details about user preferences, settings, and customizations applied to the software.
Collection of Customer Data by Whiteboard:	Account Information: When using Whiteboard, users may sign in with their Microsoft account or their organization's Office 365 account. Microsoft collects basic account information, such as the user's name, email address, and profile picture. • **Usage Data:** Microsoft collects data on how users interact with Whiteboard, including the features they use, the duration of their sessions, and the frequency of their interactions with the app. This information helps Microsoft understand user behavior and improve the application's functionality. • **Whiteboard Content**: Microsoft stores the content created within Whiteboard, such as drawings, text, images, and other objects. This data is used to enable

Category	Microsoft Whiteboard
	collaboration, sync data across devices, and provide users with access to their whiteboards from any device. • **Collaboration Data**: When users collaborate on a whiteboard, Microsoft may collect data about the participants, such as their names, email addresses, and roles within the collaboration. This information is used to facilitate the sharing of whiteboards and manage permissions. • **Device and Technical Information**: Microsoft may collect information about the user's device, operating system, browser, and other technical details to optimize the Whiteboard experience and troubleshoot any issues. • **Diagnostic Data:** Microsoft collects diagnostic data to maintain and improve the performance, security, and reliability of Whiteboard, as previously mentioned in the context of Microsoft products and services. This may include data related to device information, application data, performance data, network information, and error reporting. • **Feedback**: Users can voluntarily provide feedback about Whiteboard through surveys, feedback forms, or other means. This data helps Microsoft understand user needs and improve the application accordingly.
Data Collected and/or Processed by Whiteboard:	Microsoft Whiteboard collects and processes several types of data to provide its services, facilitate collaboration, and improve user experience. • **Account Information**: When using Whiteboard, users may sign in with their Microsoft account or their organization's Office 365 account. Microsoft collects basic account information, such as the user's name, email address, and profile picture. • **Usage Data:** Microsoft collects data on how users interact with Whiteboard, including the features they use, the duration of their sessions, and the frequency of their interactions with the app. This information helps Microsoft understand user behavior and improve the application's functionality. • **Whiteboard Content**: Microsoft stores the content created within Whiteboard, such as drawings, text, images, and other objects. This data is used to enable

Category	Microsoft Whiteboard
	collaboration, sync data across devices, and provide users with access to their whiteboards from any device. • **Collaboration Data**: When users collaborate on a whiteboard, Microsoft may collect data about the participants, such as their names, email addresses, and roles within the collaboration. This information is used to facilitate the sharing of whiteboards and manage permissions. • **Device and Technical Information:** Microsoft may collect information about the user's device, operating system, browser, and other technical details to optimize the Whiteboard experience and troubleshoot any issues. • **Diagnostic Data:** Microsoft collects diagnostic data to maintain and improve the performance, security, and reliability of Whiteboard. This may include data related to device information, application data, performance data, network information, and error reporting. • **Feedback:** Users can voluntarily provide feedback about Whiteboard through surveys, feedback forms, or other means. This data helps Microsoft understand user needs and improve the application accordingly.
Personal Information Collected:	Microsoft Whiteboard collects some personal information to provide and enhance its services, maintain a seamless user experience, and facilitate collaboration. The PI may include: • **Account Information**: When users sign into Whiteboard using their Microsoft account or their organization's Office 365 account, Microsoft collects basic account information such as the user's name, email address, and profile picture. • **Collaboration Data**: When users collaborate on a whiteboard, Microsoft may collect personal data about the participants, such as their names, email addresses, and roles within the collaboration. This information is used to facilitate the sharing of whiteboards and manage permissions. • **Device and Technical Information**: Microsoft may collect information about the user's device, operating system, browser, and other technical details. While this information may not directly identify an individual, it could be considered personal information under certain privacy regulations.

Category	Microsoft Whiteboard
	• **Feedback**: Users can voluntarily provide feedback about Whiteboard through surveys, feedback forms, or other means. This data may include personal information if users choose to share it.
Customer Data Storage Location:	When users create and collaborate on whiteboards, the content is saved to Microsoft's cloud storage, specifically in Azure and/or OneDrive, depending on the user's account type. • **For personal Microsoft accounts**, the Whiteboard data is saved to the user's OneDrive storage. • **For users with Office 365 accounts** through their organization, the data is saved to the organization's OneDrive for Business storage or SharePoint Online. In Canada, Microsoft has two data center regions: • Canada Central: Located in Toronto, Ontario • Canada East: Located in Quebec City, Quebec
Built-In Integrations:	Microsoft Whiteboard is seamlessly integrated with the following Microsoft applications: • **Microsoft Teams:** Whiteboard is integrated within Microsoft Teams, allowing users to access and collaborate on whiteboards during team meetings, calls, or chats. Users can create new whiteboards or open existing ones directly within the Teams interface, making it easy to brainstorm, discuss, and visualize ideas in real-time. • **Office 365:** Whiteboard is part of the Office 365 suite, and users with an Office 365 account can access the application across multiple devices and platforms. The integration also enables users to import Office documents, such as PowerPoint slides or Word documents, onto the whiteboard canvas for annotation and collaboration. • **OneDrive and SharePoint**: Whiteboard data is saved to OneDrive (for personal Microsoft accounts) or OneDrive for Business and SharePoint Online (for Office 365 accounts). This integration allows users to access, edit, and share their whiteboards securely from any device with an internet connection. • **Microsoft Outlook**: Users can create and share whiteboard links through Microsoft Outlook, allowing

Category	Microsoft Whiteboard
	collaborators to join a whiteboard session directly from a calendar event or email invitation. • **Windows Ink Workspace:** On Windows devices, Whiteboard is integrated with Windows Ink Workspace, providing a seamless drawing and writing experience using a digital pen or touch input. • **Immersive Reader:** Whiteboard supports Microsoft's Immersive Reader, a tool designed to improve reading comprehension and accessibility. Users can leverage the Immersive Reader on text elements within Whiteboard to adjust text size, spacing, and background color, or to enable text-to-speech capabilities.
Optional Integrations/ Connections Requiring Configuration:	None known at this time, but there are workarounds that would support collaboration, for example, users could leverage automation tools like Zapier or Power Automate to create custom workflows that connect Microsoft Whiteboard to other applications or services. For example, you could set up an automated workflow to save exported whiteboard images to a specific folder in Google Drive or Dropbox.
Activity Logging - End-user controls:	Does not appear to be any end-user controls.
User Activity Reports:	Does not appear to have user activity reports specific to Whiteboard. However, the customer 's Office 365 administrator can monitor user activities across various Office 365 services, including Whiteboard through the Office 365 Audit Logs.
Auditing:	As included in Office 365 Audit Logs: • **Whiteboard Creation**: When a user creates a new whiteboard. • **Whiteboard Access**: When a user accesses or opens an existing whiteboard. • **Whiteboard Modification**: When a user modifies a whiteboard, such as adding, editing, or deleting content. • **Whiteboard Sharing**: When a user shares a whiteboard with other users or changes sharing permissions. • **Whiteboard Deletion:** When a user deletes a whiteboard.
Security Compliance:	Relevant Microsoft compliance:

Category	Microsoft Whiteboard
	• ISO/IEC 27001: Microsoft has achieved ISO/IEC 27001 certification for its Information Security Management System (ISMS). • SOC 1, SOC 2, and SOC 3: Microsoft 365 services undergo Service Organization Controls (SOC) audits and have achieved SOC 1, SOC 2, and SOC 3 compliance, demonstrating strong internal controls and security practices. • ISO/IEC 27018: Microsoft Forms is compliant with ISO/IEC 27018, an international standard that establishes guidelines for protecting Personally Identifiable Information (PII) in public cloud environments. • NIST Cybersecurity Framework: Microsoft aligns with the NIST Cybersecurity Framework and implements its guidelines across applications and services to ensure a robust security posture.
Privacy Safeguards:	Whiteboard shares privacy safeguards with other Microsoft applications, such as access controls, data encryption, and data retention policies. A unique privacy safeguards in Whiteboard is that it supports real-time collaboration, meaning that multiple users can work on the same Whiteboard in real-time. This feature includes controls to manage user access and sharing, such as the ability to invite specific users to collaborate on a Whiteboard and to restrict access to the Whiteboard to only certain users or groups.
Potential Privacy Risks:	Potential privacy risks inherent in Whiteboard include the following: • **Unauthorized Access:** If a whiteboard's sharing permissions are not configured properly, unauthorized users might access the content. This risk can be mitigated by regularly reviewing sharing settings and limiting access to only those who need it. • **Data Storage and Transmission**: Whiteboard data is stored on Microsoft's cloud infrastructure, which can be a concern for organizations with strict data residency requirements. However, Microsoft employs strong encryption for data at rest and in transit and follows robust security standards to protect stored data.

Category	Microsoft Whiteboard
	• **Data Collection and Usage**: Microsoft collects certain data from Whiteboard users, including personal information, usage data, and whiteboard content. While Microsoft takes steps to anonymize and aggregate data, there may still be concerns about data privacy and how the collected information is used. • **Third-Party Integrations**: Although Whiteboard has limited third-party integrations, users may export data or share whiteboard links through other platforms, which may introduce privacy risks depending on the security of those platforms. • **Human Error**: Users may inadvertently share sensitive information or create content on Whiteboard that violates privacy guidelines, such as discussing personally identifiable information (PII) or confidential company data. This risk can be mitigated through user training and awareness programs.
Privacy Risk Mitigations:	Privacy risk remediations specific to Whiteboard can be shared between VIU administrators and VIU end-users. Vancouver Island University Administrator Mitigations: • **Access Control and Sharing Permissions:** Organizations should enforce strict access control policies for Whiteboard, ensuring that only authorized users can access and collaborate on whiteboards. This can be done through proper configuration of sharing settings and user access permissions in the Microsoft 365 Admin Center. • **Data Residency and Compliance:** To address data storage and transmission concerns, organizations can review Microsoft's data storage practices and configure data residency settings in accordance with their specific requirements. Additionally, organizations should ensure compliance with relevant data protection regulations, such as GDPR, by implementing appropriate policies and procedures. • **Monitoring and Auditing**: Organizations can enable and review Office 365 Audit Logs to monitor user activities within Microsoft Whiteboard. Regular monitoring helps identify any unauthorized access, data leakage, or

Category	Microsoft Whiteboard
	suspicious behavior, allowing organizations to take corrective actions promptly. - **User Training and Awareness:** Providing regular training and awareness programs for employees can help reduce the risk of human error. This includes educating users about best practices, the importance of data privacy, and how to identify and report potential privacy risks. **End-User Mitigations:** - **Secure Sharing:** Users should always verify the recipients and sharing permissions before sharing a whiteboard, ensuring that only intended collaborators have access to the content. Additionally, users should avoid sharing sensitive information through public or unsecured channels. - **Password Protection**: Users should use strong, unique passwords for their Microsoft accounts to prevent unauthorized access. Implementing multi-factor authentication (MFA) can further enhance account security. - **Exporting Data:** When exporting whiteboard data to third-party applications or services, users should consider the privacy risks associated with those platforms and follow their organization's guidelines for sharing or transferring data. - **Content Creation**: Users should avoid creating or sharing content on Whiteboard that contains personally identifiable information (PII) or confidential company data, in compliance with their organization's privacy policies. - **Reporting Incidents**: If users identify potential privacy risks or experience unauthorized access to their whiteboards, they should promptly report the incident to their organization's IT or security team.
Other Key Links:	- Getting started with Microsoft Whiteboard - Microsoft Support - Whiteboard help & learning (microsoft.com) - Tips and Tricks for Microsoft Whiteboard - Microsoft Support - Guides to Microsoft Whiteboard - Microsoft Support - Use mouse, keyboard, and pen in Whiteboard - Microsoft Support - Share a whiteboard in Microsoft Teams - Microsoft Support - Insert templates in Whiteboard - Microsoft Support

Category	Microsoft Whiteboard
	• Microsoft Privacy Statement – Microsoft privacy • Microsoft Trust Center Overview | Microsoft Trust Center

END