

Douglas College Privacy Impact Assessment Form

Part 1 - General

1. Unit and Program Area

Faculty/Department/ Division	CEIT
Program Area	Infrastructure Services

2. Contact Position and/or Name, Telephone Number and E-Mail Address.

Name	Dan Georgescu
Title	Manager, Infrastructure Services
E-Mail	georgescud@douglascollege.ca

3. Description of the Program, System or Initiative being assessed.

This privacy impact assessment (PIA) assesses the use of Microsoft Teams for students at Douglas College. Teams for students supports collaboration between students and in the learning environment. Teams is a communication platform, part of the O365 ecosystem, which provides chat, videoconferencing, file storage, and application integration.

4. Scope of this PIA

This PIA examines the collection, use, disclosure, security, and storage of personal information in the College's deployment of Microsoft Teams for students. This PIA does not cover other O365 products.

5. Related PIAs

N/A

6. Elements of Information or Data Collected

Information Collected

Information Type	Information Collected from Account Holder	Information Collected from Non-Account Holder
1. Azure active directory data	Y	N
2. Teams data	Y	N
3. Metadata	Y	N

Information Provided to Third Parties

7. Storage or Access outside Canada

This document is marked **INTERNAL**. (May be shared with authorized external parties.)

Douglas College Privacy Impact Assessment Form

Customer data remains in Canada. Azure Active Directory data is stored outside of Canada and there is no option for this data to be stored in Canada. Azure Active Directory data consists of student names and email addresses – this is not considered sensitive personal information.

8. Data-linking Initiative?

No

9. Common or Integrated Program or Activity?

No

10. Risk Classification Level

This is a medium risk project. Only Azure Active Directory data is stored and processed outside of Canada, other customer data remains in Canada, and this information is not considered sensitive. There is clear legal authority for the collection, use, and disclosure of student information and the initiative relates to the core mission of the College. There is inherent risk given the large scale of this initiative and the potential for a significant amount of personal information to be shared.

Part 2 – Protection of Personal Information

11. Personal Information Flow Diagram/ Table

<i>Description/Purpose</i>	<i>Type</i>	<i>FIPPA Authority</i>
1. Student information used to populate Active Directory and enable Teams.	Collection	FIPPA s. 26(c)
2. Customer data is uploaded to Microsoft Teams.	Use/disclosure	FIPPA s. 26(c)
3. User shares data in Teams with others	Disclosure	FIPPA s. 33 (2) (d)

12. Risk Mitigation Table

Risk Mitigation Table			
<i>Risk</i>	<i>Mitigation Strategy</i>	<i>Likelihood</i>	<i>Impact</i>
1. PI Stored/accessible outside of Canada	1. Microsoft customer data is stored in Canada. 2. Active Directory data stored outside of Canada is student contact information (e.g., name and email) which is not considered sensitive.	Low	Low

Douglas College Privacy Impact Assessment Form

2. Excessive collection of PI	1. Ensure minimal collection of data for account creation.	Medium	Medium
3. Unauthorized retention or deletion of PI	1. Develop retention policies for teaching and learning environments. 2. Processes required for removal of individuals from Teams if memberships are based on course enrolment.	Medium	Medium
4. Unauthorized disclosure of PI	1. Processes required for removal of individuals from Teams if memberships are based on course enrolment. 2. Review of configuration settings on a regular basis to ensure PI is not inadvertently exposed by configuration choices.	Medium	High

13. Collection Notice/Consent

Collection Notice

N/A. There is no specific collection notice for the use of Teams. It is assumed that for teaching and learning use cases the information has been collected in a FIPPA compliant manner, using collection notices where appropriate (e.g., course syllabus).

Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

N/A. Data, with the exception of Active Directory data, is hosted and stored in Canada. Azure Active Directory data is not considered sensitive.

Part 3 – Security of Personal Information

14. Physical Security Measures

Microsoft's O365 services, including Teams, are hosted at data centers owned and managed by Microsoft. Physical protection of these data centers is managed by Microsoft and is reported in their SOC 2 type II audits and in other security reports and reviews. Microsoft documentation has been reviewed by the Associate Director Information Security who signs off on appropriate security measures as part of this PIA.

15. Technical Security Measures

Microsoft documentation has been reviewed by the Associate Director Information Security who signs off on appropriate security measures as part of this PIA. Microsoft's SOC 2 Type II report specifies security controls which fall outside its remit in regards to maintaining the security and integrity of customer data and are the responsibility of the College.

Douglas College Privacy Impact Assessment Form

16. Security Policies, Procedures and Standards

Microsoft's published information security and standards, and governance and compliance processes apply to Microsoft's delivery and provisioning of O365 and related MS Azure services. Douglas College's information security standards and policies apply to all files and content of the files that users upload to and share via Teams.

Part 4 – Accuracy, Correction and Retention

17. Updating and Correcting Personal Information

Students are able to make updates or changes to certain personal information through Enrolment Services and the Banner system.

18. Decisions Made That Directly Affect an Individual

The use of Teams does not necessarily lead to decisions which directly affect an individual as contemplated by s. 31 of FIPPA.

19. Records Retention and Disposal

The development of records retention and disposal procedures will follow implementation.

Part 5 – Further Information

20. Systematic Disclosures?

N/A

21. Access to PII for Research or Statistical Purposes?

N/A

Part 6 – Access and Privacy Manager Comments

22. Information or Materials Reviewed

- Microsoft documentation and policies
- The Teams implementation group met several times and received verbal updates that informed this PIA.

23. Analysis and Decision

This PIA has determined that Teams implementation can be delivered in compliance with FIPPA and College policies. Updates may be required should changes be made to implementation and service delivery. Teams is a service that may store a large amount of personal information, some of which may be highly sensitive, so

This document is marked **INTERNAL**. (May be shared with authorized external parties.)

Douglas College Privacy Impact Assessment Form

there is inherent risk in its implementation. See below for conditions of approval.

24. Conditions of Approval

- Students do not have access to contact information for other students (i.e., there is no global disclosure of all student profiles). Students need to know email address of other students to add them to a Team (NB: this was a configuration decision by project team and is not necessarily due to privacy concerns).
- Implementation of retention and disposition process for Azure Active Directory data for students.
- Implementation of retention and disposition process for Teams customer data.
- Project team must document configuration settings to ensure security and privacy requirements are met.
- Any contemplated changes to or use of this software that differs from the description provided by this PIA (e.g., in the collection, use, disclosure or storage of personal information) must be reviewed by the Privacy Office for compliance with FIPPA.

Part 7 - Signatures

The undersigned confirm that they have taken reasonable steps to confirm that the contents of this PIA are accurate and complete.



AVP, Technology and CIO

December 20, 2021

Date

authorization on file

Associate Director, Information Security

December 15, 2021

Date



Privacy Officer

December 20, 2021

Date