

PIA02077 – Padlet

PIA REVIEW – EXECUTIVE REPORT



PREFACE

This document forms part of UBC Safety and Risk Services (SRS) PrISM’s internal documentation for support and administration of the Privacy Impact Assessment (PIA) Review Process. In particular, it documents the final report of the specified PIA review.

This segment serves to provide and record document control capabilities for this document.

Controlled Document

The template and final report documents are controlled documents. The master electronic versions of each reside on the SRS TeamShare S-drive. Any copies or versions not provided directly by the SRS PrISM team, or which have a broken chain of custody, are not to be considered as official copies.

Document Control

The following sub-sections provide a record of the base document template revision history and control.

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Christian Stockman	Safety and Risk Services	Privacy and Information Security Risk Advisor

Figure 1 - Major Document Revision Approval History

TEMPLATE REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
1.0	2021-10-28	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2021-10-28	Ian Linkletter	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

PREFACE 1

 Controlled Document 1

 Document Control 1

 CONTRIBUTORS..... 1

 TEMPLATE REVISION HISTORY 1

 TEMPLATE REVISION APPROVAL 1

TABLE OF CONTENTS..... 2

TABLE OF FIGURES 4

PART 1: GENERAL INFORMATION & OVERVIEW 1

 1.1 Executive Summary 1

 1.2 Description of the Program, System, Application, or Initiative Assessed..... 1

 1.3 Scope of PIA 1

 1.4 Elements of Information or Data..... 1

 1.5 Storage or Access Outside of Canada (including back-ups and recovery)..... 1

 1.6 Data-Linking Initiative..... 1

 1.7 Is this a Common or Integrated Program or Activity?..... 1

PART 2: PROTECTION OF PERSONAL INFORMATION 2

 2.1 Personal Information Flow Diagram / Table 2

 2.2 Risk Mitigation Table..... 3

 2.3 Collection Notice 4

 2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any) 4

 2.5 Consent Withheld Procedure..... 4

PART 3: SECURITY OF PERSONAL INFORMATION 5

 3.1 Physical Security Measures 5

 3.2 Technical Security Measures..... 5

 3.3 Security Policies, Procedures, and Standards..... 5

 3.4 Tracking Access / Access Controls..... 5

PART 4: ACCURACY, CORRECTION, AND RETENTION 5

 4.1 Updating and Correcting Personal Information 5

 4.2 Decisions That Directly Affect an Individual..... 5

 4.3 Records Retention and Disposal..... 5

PART 5: FURTHER INFORMATION	6
5.1 Systematic Disclosures of Personal Information	6
5.2 Access for Research or Statistical Purposes	6
5.3 Other Applicable Legislation and Regulations.....	6
PART 6: ACCESS AND PRIVACY MANAGER COMMENTS.....	6
6.1 Information or Materials Reviewed	6
6.2 Analysis and Findings	6
6.3 Conditions of Approval.....	7
6.4 Review and Distribution	7

TABLE OF FIGURES

Figure 1 - Major Document Revision Approval History	i
Figure 2 - Document Revision History and Revision Summary	i
Figure 3 - Major Document Revision Approval History	i
Figure 4 - Risk Mitigation Table.....	3

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

The UBC Faculty of Education (FoE) uses Padlet, a SaaS tool hosted on the Google Cloud Platform that allows real-time collaborative web platform in which users can upload, organize, and share content to virtual bulletin boards called "padlets" (similar to a text box). At UBC, padlets are embedded as iframes within the Canvas learning management system (LMS). Students interacting with the padlets when they use the LMS but there is no integration otherwise, and Padlet does not access Canvas data. Students register for an account with Padlet and are then able to post content and respond to discussions. Instructors will use content posted in padlets within their courses to grade online participation.

1.2 Description of the Program, System, Application, or Initiative Assessed

Instructors at the Faculty of Education have been using Padlet frequently in their courses over the past year. This is because it adds a new level of interaction to online courses, facilitating discussions in a way that's more visual than a Canvas Discussion board. However, before we promote and officially support this tool, we would like a PIA conducted on Padlet.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is **4 - High**.

The residual risk classification level of this PIA submission at closure is **3 - Medium**.

1.3 Scope of PIA

The scope of this PIA is the implementation of SurveyMonkey Apply for direct use by UBC faculty, staff, students and other third parties who are authorized to use these products and services on behalf of UBC.

1.4 Elements of Information or Data

Padlet doesn't require students to create an account or add their names in order to contribute to a board. An email address is mandatory for users to use Padlet as registered users. Other data is optional like name and username can be aliases. Optional information may be provided, including a profile photo. Padlet can also be used in a guest mode where registration is not required. Instructors often will ask students to include their first names in posts in order to grade participation. Users are actively discouraged from providing real names and personal information beyond the first name or alias for grading purposes.

Padlet uses tracking cookies and Google Analytics to gather personal information about users and their devices, including IP address (geolocation).

1.5 Storage or Access Outside of Canada (including back-ups and recovery)

Padlet stores personal information on servers outside of Canada in the USA. Services are primarily hosted in Google Cloud. Backups are maintained on AWS servers.

1.6 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under s.(36) of FIPPA.

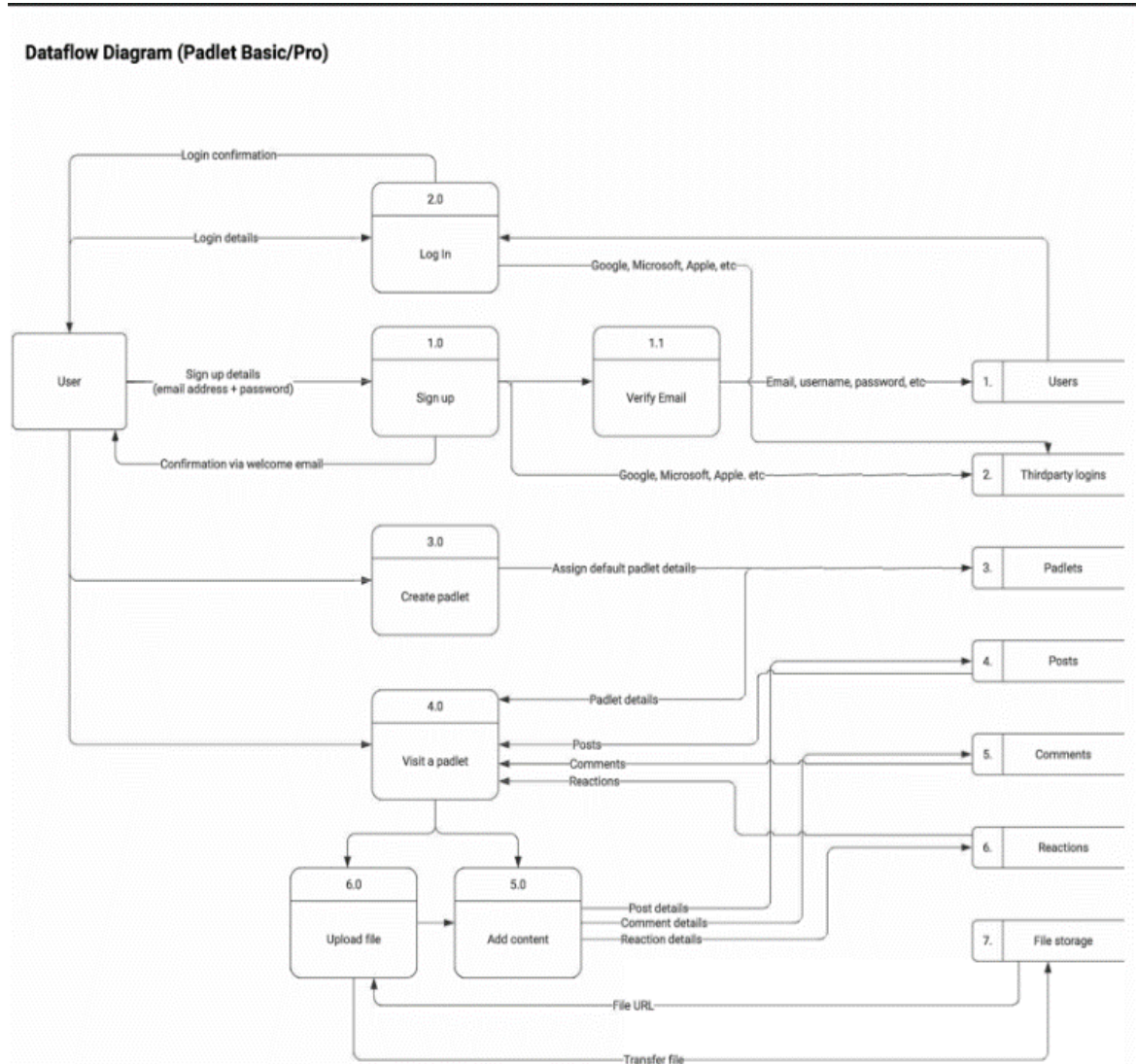
1.7 Is this a Common or Integrated Program or Activity?

This project is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

The following data flow was supplied.



2.2 Risk Mitigation Table

The following table indicates the associated risk levels as applicable and the potential or intended mitigation steps.

Category: Privacy					
Risk	Ref#	Inherent Likelihood	Inherent Impact	Response	Residual Risk
Disclosing to or allowing unauthorized users access	RK0020786	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Personal information will not be disclosed to or shared with third parties internal or external to UBC. Padlet will have access to all information on the boards. The rest of the students in the course and the instructor will also be able to see other student contributions within Canvas. Padlet contents remain with the Canvas learning management system. No integrations exist between Padlet and Canvas, as the Padlet contents exist independently of Canvas (embedded as iframes).				
Retaining PI longer than necessary	RK0020930	4 - High	3 Significant	Mitigate	2 - Low
	Mitigation Plan: The FoE has committed to retaining personal information for the one-year minimum required time under FIPPA, and to meet academic appeal requirements. The FoE should regularly request Padlet to dispose of all unnecessary personal information beyond the one-year mark, and to confirm that this has been done. The FoE is encouraged to develop a formal records retention plan in conjunction with the UBC Records Management Office.				
Inadequate third-party information sharing controls	RK0020785	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Users have the ability to register for Padlet using Google, Apple, or Microsoft login credentials. Use of these services is discouraged, as it will link Padlet access to third party vendors and enables uncontrolled collection of additional personal information subject to the terms and conditions of these services.				
Category: Security					
Risk	Ref #	Inherent Likelihood	Inherent Impact	Response	Residual Risk
Weak or absence of technical security controls	RK0020931	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: FoE to work with the vendor to implement password minimum length of 10 characters with complexity to comply with UBC Password Standards. Alternatively, users can manually set their passwords to follow the UBC password requirements.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

Recommended collection notice:

"Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA). This information will be used for the purpose of enabling your participation in UBC courses and evaluating your participation. By submitting your personal information, you are consenting to the storage of this information on a secure server located in the United States. Questions about the collection of this information may be directed to <INSERT EMAIL>@ubc.ca."

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

Students using Padlet will be required to consent to having their personal information stored outside of Canada. Alternatively, students may use an alias name and email address or their @students.ubc.ca email address for registration.

2.5 Consent Withheld Procedure

Students not wishing to use Padlet or who do not wish to have their personal information stored outside of Canada will be presented with an alternative option at the start of each term to enable their participation on the course.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards)

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

Padlet has completed a HECVAT and is targeting SOC 2 attestation in 2022.

3.4 Tracking Access / Access Controls

The vendor will have access to all information on the padlet boards within the Canvas LMS. The rest of the students in the course will also be able to see other student contributions, as would instructors. Personal information pertaining to registered users would be available to UBC FoE account administrators. Third party sub-processors are used to provide some services, and will have access to personal information (i.e. email notification and processing).

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not applicable

4.2 Decisions That Directly Affect an Individual

This project captures personal information that directly affects an individual. Under s.(31)(b) of FIPPA, personal information used to make a decision about an individuals must be retained for at least one year.

4.3 Records Retention and Disposal

This project is required to comply with UBC Records Management Policies.

The FoE has confirmed personal information is retained for a year and a day at minimum to comply with academic appeal requirements. Padlet has confirmed they destroy all personally identifiable data when it is no longer needed for the purpose for which it was obtained. For individual accounts, users can request an account deletion from their settings panel. For schoolwide accounts, account owners can request for account deletion and we will delete all PII within 60 days. It is recommended that the FoE develop a formal records retention policy to govern disposition of Padlet data

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

This project does not involve the disclosure of personal information for research or statistical purposes as contemplated under s.(35) of FIPPA.

5.3 Other Applicable Legislation and Regulations

This project is not subject to other applicable legislation or regulations.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

The following documentation was reviewed in the context of this PIA. The provided information was deemed reasonable to provide an understanding of operating privacy and security controls:

Information Reviewed	Date Received
Padlet Dataflow Diagram.jpg	2021-10-22 19:35:55
Padlet HECVAT.xlsx	2021-09-11 01:56:55
Padlet Privacy Policy.pdf	2021-09-11 01:56:55
Padlet subprocessor list.xlsx	2021-10-22 18:31:12
Padlet technical physical organisational measures.pdf	2021-09-11 01:56:55
Padlet Terms of Service - Schools.docx	2021-09-11 01:56:55
Padlet Terms of Service.pdf	2021-09-11 01:56:55

6.2 Analysis and Findings

The information provided for the review has established that Padlet and the associated use-case, as presented by the UBC Faculty of Education, can be used in the proposed manner in compliance with FIPPA and UBC policies and standards.

The following are the key factors in that determination:

- Personal information is collected, stored, and accessed within Canada, and outside of Canada with appropriate consent;
- Personal information is not disclosed to third parties external to authorized UBC staff members and the vendor's support teams;
- Access to the service requires use of a valid login credentials with appropriate access authorities;
- Information is kept secure during transmission and at rest.

Based on our understanding of the collection, use, disclosure, and retention of personal information, our review noted the key privacy and information security risks and the risk mitigation plan is recommended and provided to the project. The project has agreed and implemented the recommended remediation actions as outlined in the risk mitigation plan to minimize risk exposures and to comply with the FIPPA requirements and UBC Information Security Standards. Accordingly, Padlet can be used as proposed subject to the conditions outlines in the following section.

6.3 Conditions of Approval

Our review has concluded that there are no significant privacy or information security risks introduced by this project. We do recommend, however, that the project ensure that it continues to fully comply with BC FIPPA legislation and the UBC Information Security Standards.

6.4 Review and Distribution

This refers to the report approval process. The Owner is accepting the accuracy of the data provided to PRISM for this review and the risk responses. The Owner is responsible for the on-going operational activities and must ensure that this project continues to meet legislative and legal requirements, along with Information Systems Policy (SC14) requirements. Any change in PI collection or use will require new PIA.

Assessment Acceptance
Natasha Boskic

This refers to the report distribution, including Requestor, Project Manager, Owner, and assigned Risk Advisor.

Distributed To
Requestor: Ian Linkletter, Learning Technology Specialist Project Manager: Ian Linkletter, Learning Technology Specialist Owner: Natasha Boskic, Director, Learning Design Risk Advisor: Christian Stockman, Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2021-07-06 14:39:12	2021-10-27 15:55:14