PIA01538 — DAE ThankView – Fundraising Tool

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

In light of the COVID pandemic and continued work from home/physical distancing requirements, fundraising tools are becoming more and more important to the line of business and this is now being prioritized. DAE Development is implementing a new fundraising tool to enhance contact-free communication with donors.

1.2 Project Description

ThankView is utilized as a tool to facilitate virtual donor engagement through email communications and appreciation videos. These communications are designed to inform both prospective and existing donors about fundraising events. The information used for these communications is handled according to UBC's data governance policies to ensure privacy and compliance with legal standards. Participation in thank you videos by UBC employees and students is voluntary and managed under strict consent guidelines.

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 4 – **High**.

1.3 Scope

Functions utilized in ThankView including email capability.

1.4 Data Elements

UBC collects essential personal information for employees and students participating in the program, which may include contact details and multimedia elements for identification purposes.

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

Data related to the project is hosted internationally in alignment with UBC's data management policies.

1.6 Data-Linking Initiative

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

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 FIPPA Schedule 1.

1.8 Related PIAs

PIA01539 - DAE THANKVIEW (2/2) - Production & Distribution of Videos

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram/Table

None provided.

2.2 Risk Mitigation Table

Privacy Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Not ensuring individuals are informed about collection	RK0020262	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to implement the proper privacy and consent notification (using Consent to Use of Image) and obtain consent from an individual prior the project records fundraising or thank you videos of the individual.				
Disclosing to or allowing unauthorized users access	RK0020265	4 - High	4 - Major	Mitigate	4 - High
	Mitigation Plan: Appropriate risk mitigation measures are implemented to align with privacy laws and UBC's data security and data governance policies.				
Retaining PI longer than necessary	RK0020266	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: The project to ensure Thank View follow the DAE's standard retention requirement of seven years.				
PI stored / accessible outside of Canada	RK0020261	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project has agreed and worked with ThankView to address initial concerns over disclosure of personal information outside Canada: • to host UBC production data, backups, and caches at AWS Canada location. • to ensure that ThankView's support team be assigned only with a temporary access within the minimum period of time necessary to complete the implementation, maintenance and trouble-shoot. • to have its US-based email processor (Postmark) to retain data only in Canada.				
Disclosing PI not authorized by legislation	RK0020264	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project has ensured appropriate security agreements are in place with external service providers before granting access to personal or otherwise sensitive information held by UBC, in compliance with relevant legislation.				

Security Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of administrative security controls	RK0020267	4 - High	4 - Major	Mitigate	4 - High
	Mitigation Plan: Per the current licensing model, three user accounts are given. The project to assign each user account to an individual and no sharing of account be permitted.				

2.3 Collection Notice

UBC employees and students previously provided consent for their contact information to be used within the scope of their initial interaction with the LINKS database. For participation in fundraising or thank you videos, a distinct and explicit consent process will be conducted, adhering to legal standards for personal information collection. This process will include providing individuals with a clear personal information collection notice that outlines the legal authority for collection, the specific purposes for which the information will be used, and details for whom to contact for further clarification regarding privacy concerns. Individuals are encouraged to contact the DAE Development team directly should they have questions about the use of their data or wish to discuss privacy protections.

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

Not applicable, the project has committed to work with ThankView to disclose, access and store PI in Canada to comply with the FIPPA legislation.

2.5 Consent Withheld Procedure

Presenting in the fundraising or thank you videos is on a voluntary basis. UBC employees and students has the right to withhold their consent and not participating in the videos if they wish to do so.

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).

3.4 Tracking Access/Access Controls

Access to the system is restricted to designated personnel within UBC DAE, with strict controls based on assigned roles.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

The donor name and email address obtained from the UBC staff directory and LINKS database would be pre-validated by the Annual Giving Office.

4.2 Decisions That Directly Affect an Individual

Not applicable.

4.3 Records Retention and Disposal

The DAE's standard retention periods which is 7-years on DAE fundraising database and file repositories would be followed. If data is related to specific gifts received by the University, then data retention past this period may be required for purposes of fundraising, gift administration (such as tax receipting), adhering to CRA guidelines or other compliance requirements. If a specific request comes in for removal before the end of the retention period, the DAE IT and/or UBC IT team would provide data destruction support.

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 FIPPA s. (35).

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 provided information was deemed reasonable to provide an understanding of operated controls.

6.2 Analysis and Findings

This project results in no additional collection, use or storage of personal information by UBC. However without adequate control it does result in an increased risk of disclosure of personal information. Controls to mitigate this risk are stipulated within this PIA and are considered sufficient to mitigate the risk.

6.3 Conditions of Approval

Our review has concluded there are no significant privacy or security risks introduced by this project however we do recommend the project implement the following mitigation strategy to fully comply with FIPPA and UBC Security Standard.

6.4 Review and Distribution

The Minister of Citizens' Services Direction 2-21, *Privacy Impact Assessment Directions* requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s. D8).

Accountability is maintained by the role or position, regardless of who fills the role.

Under UBC Policy SC14, Administrative Heads of Unit are responsible for:

- ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
- ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
- authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
- renewing, retiring, and revoking User authorizations within their area of responsibility.

Holding accountability for the privacy risks of this initiative includes:

- reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;
- ensuring accountability is transferred to any individual who assumes this role;
- if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the PIA team is engaged, and if necessary, completing a PIA update; and
- understanding what your privacy obligations are, and if not, following up with the PIA team.

Assessment Acceptance
Sarah Koh

Distribution
Requestor: Sarah Koh **Project Manager**: Sarah Koh **Owner**: Sarah Koh **Risk Advisor**: Pimkae Saisamorn

PIA Request Submission	Report Completion
2020-06-02	2020-09-16