PIA02599 — Arts Mailing List System

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

The Arts Mailing List initiative is designed to streamline the creation and management of mailing lists within the Faculty of Arts at UBC. Utilizing Workday API's, this project will systematically collect personal information of staff and faculty members, including but not limited to full names, email addresses, and other role-, team-, or department-related attributes, to accurately assemble these lists.

This report evaluates various risks associated with the project. These encompass potential challenges such as such failure to adequately inform individuals about the collection and use of their personal information, utilization of personal information for purposes not originally consented to, over-collection of personal information, insufficient governance measures, lack of retention controls, and deficiencies in technical security measures.

To ensure the project's success and compliance, it must adhere to several critical frameworks and policies, including the Freedom of Information and Protection of Privacy Act (FIPPA), the Canadian Anti-Spam Legislation (CASL), UBC Policy SC14, UBC Information Security Standards (ISSs), and the UBC Records Management Policies. Furthermore, any significant change to the project's scope or its application will necessitate an amendment to the PIA.

1.2 Project Description

This project aims to establish a system for the Faculty of Arts, facilitating the creation and ongoing management of mailing lists. The primary objective is to ensure the efficient distribution of email communications to staff and faculty members. Additionally, the system will enable the exportation and importation of these lists into Envoke, supporting the dissemination of optional Departmental Newsletters to relevant individuals within each Department or Unit. It is important to note that any requests to unsubscribe will be processed manually by the Arts communication team, utilizing the Sympa platform.

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

The scope of this report will cover both information security and privacy risks related to the use and implementation of Sympa by UBC's Faculty of Arts. At this time Sympa will not be used for establishing mailing lists for students.

1.4 Data Elements

Data Elements for Faculty/Staff:

- General Information: Full Name, Email Address
- HR Attributes for List Creation: These include identifiers related to job profiles, positions, departments, and employment status within the organization, which are used to manage and authenticate user access according to their operational roles and active status.

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

Personal information is stored within Canada and hosted on UBC Arts IT's EduCloud environment.

1.6 Data-Linking Initiative

None provided

1.7 Is this a Common or Integrated Program or Activity?

None provided

1.8 Related PIAs

Similar PIAs include those completed for commonly used mass emailing tools such as; CyberImpact, Envoke, and UBC Sendy.

Sympa, which is used by the Faculty of Applied Sciences, predates UBC's PIA process. Therefore, all relevant mitigations identified in this report should be applied to their use of the platform.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram/Table

1. A nightly automated process triggers the Workday API to extract necessary data for staff and faculty in the Faculty of Arts, utilizing specific organizational filters.
2. Relevant data such as names and email addresses are organized into lists according to additional attributes like the individual's academic or professional details.
3. Once lists are compiled, any temporary attributes used during processing are not stored but exist only transiently in the system's memory.
4. List owners from Arts Communication periodically transfer these lists into a CSV file, which are then uploaded to Envoke for email distribution. Each upload replaces the previous data set to ensure list accuracy.

2.2 Risk Mitigation Table

Risk	Risk Description	Mitigation Plans
Not ensuring individuals are informed about collection	Potential non-compliance due to collecting PI without informed consent, leading to a breach of trust and potential legal repercussions.	To address the risk of not ensuring individuals are informed about the collection of their information, we recommend the following measures: • Improve transparency by informing individuals when their information is added to a mailing list, clarifying the use of their personal data. • Should the mailing list serve non-mandatory purposes in the future, provide an unsubscribe option, respecting individuals' right to control their personal information. • Adhere to the requirements, including actioning unsubscribe requests within 10 days, to align the practices with legal standards.
Inadequate controls for volume of personal information	The manual process for unsubscribing poses compliance risk with the CASL, as unsubscribe requests must be actioned within 10 days.	It is critical that the Arts faculty establish and clearly communicate the responsibilities of list owners. Implement regular reviews of mailing lists to ensure ongoing compliance with CASL requirements. To further reduce this risk, especially before any expansion of use to departments beyond Communications or before including student data, automation of the unsubscribe process is strongly recommended.
Use of personal information for an alternate purpose	Employing personal information for purposes other than those for which it was originally obtained or compiled, or for uses inconsistent with that initial purpose, poses risks of non-compliance with legislation, UBC policies and standards, and could result in reputational harm.	The Arts Mailing System is designed for creating mailing lists that facilitate the distribution of mandatory emails and optional departmental/or unit newsletters to staff and faculty members within the respective department or unit. In the event future adjustments to include non-mandatory newsletters, an amendment to the current PIA will be required. This precaution ensures that any broadening in the scope of using personal information remains in strict compliance with to adhere our privacy protocols.
Weak or absence of retention controls	Retention of personal information beyond its necessary period heightens the risk associated with privacy breaches, as it increases the volume of information susceptible to unauthorized accessor disclosure.	Personal information, including names and email addresses, is scheduled for deletion immediately after the corresponding account becomes inactive in Workday. This deletion process is executed nightly, ensuring data accuracy and minimizing the risks of retaining outdated information. Data elements essential for generating mailing lists are held solely in the system's operative memory on a temporary basis. This practice is designed to ensure that personal information is not kept longer than required for its intended use, adhering to principles for data minimizing and retention.
Over collection of personal information	Collecting or granting access to more personal information than necessary for a program or activity poses a risk of non-compliance with FIPPA and UBC policies. Such practices can amplify the consequences of privacy breaches and elevate the risk of non-compliance.	The Arts IT team has implemented a practice of creating distinct service accounts for each application they develop. This ensures that each account is granted with only the essential permissions needed to access the data necessary for compiling the pre-defined mandatory mailing lists, mitigating the risk associated with the over-collection of personal information. Further to minimize over-collection, the Arts IT team has collaborated with the Enterprise Data Governance team to identify how to reduce data exposure when making API calls. It was recommended to employ the "hierarchy" filter during data access operations, limiting the scope of accessed data exclusively to individuals affiliated with the Faculty of Arts. This measure ensures compliance with the principle of data minimization.
Inadequate governance for personal information protection including policies and accountability	The potential for non-compliance arises from unclear definitions of roles and responsibilities regarding PI protection, the existence of outdated or absent policies and procedures, failure to adhere to the FIPPA and ISSs, and inconsistent or inadequate oversight of PI management processes.	Access to personal information within the mailing lists is restricted to the Arts Communication team and Arts IT system administrators. This approach guarantees that only authorized personnel have access to sensitive data, thereby safeguarding it against unauthorized use or disclosure. Additionally, a Role-Based Access Control (RBAC) matrix has been implemented, clearly outlining roles and responsibilities, with access permissions granted strictly on the principle of least privilege to minimize potential exposure. Currently, the Arts Mailing List System is used primarily for sending mandatory emails by the Arts Communication team. If the scope of use or system access changes, UBC will establish appropriate governance documentation to ensure continued protection of personal information.
Weak or absence of technical security controls	Insufficient technical security controls elevate the risk of exposing the University to potential vulnerabilities and threats, compromising data integrity and security.	This project has been designed to adhere strictly to the UBC Policy SC14 (Information Systems Policy) and the relevant UBCISSs. To ensure compliance with these standards, Arts IT has implemented the following technical controls: • The project uses advanced security technology to ensure continuous monitoring of server activities, protecting against potential security breaches. • Proactive security assessments are routinely conducted to identify and address any security vulnerabilities promptly, maintaining system integrity. • Arts IT maintains strict logging practices with a standard retention period, facilitating precise monitoring and analysis of system activities over time. • Access to systems databases is restricted to internal networks, effectively mitigating the risk of unauthorized external access. • Enhanced authentication controls are in place to ensure robust system access security.

2.3 Collection Notice

None provided.

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

None provided.

2.5 Consent Withheld Procedure

None Provided.

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 UBCISSs. It has been confirmed in previous reviews that Educloud meets these requirements.

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBCISSs. Based on the documentation provided by the project team and the completion of UBC's Application Risk Assessment, these requirements are met. A copy of this assessment is available within the PIA ticket in ServiceNow.

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

The system administration of the platform will be managed by designated administrative personnel, who will have comprehensive access for maintenance and oversight purposes. The Help Desk will oversee the authorization process for creating new operational lists.

Currently, specific team members are designated as List Masters, holding the responsibility for ensuring that lists are utilized solely for their intended mandatory purposes. As the scope of these lists may evolve, List Masters will take on further duties to maintain list usage compliance and oversee the unsubscribe mechanism.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Sympa is not recognized as the authoritative source for this data. Consequently, any inaccuracies must be rectified at the origin of the data. In this instance, corrections should be made within Workday.

4.2 Decisions That Directly Affect an Individual

This project does not capture personal information that directly affects an individual.

4.3 Records Retention and Disposal

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

When individuals are marked as inactive in Workday or removed from SIS and their associated data will be removed from the Arts Mailing List System (Sympa).

All additional attributes as noted in section 1.6 Data Elements will be handled by the system's operative memory, meaning after their temporary use to establish mailing lists they will not be retained within the system.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information as email lists will not be accessible to other departments at UBC or external parties.

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

In addition to FIPPA this project is also subject to comply with the Canadian anti-spam legislation (CASL).

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

None provided.

6.2 Analysis and Findings

Based on the project documents supplied for evaluation, it has been confirmed that the project and its corresponding use case, as described, can proceed as planned. Currently, the utilization of Sympa by the Faculty of Arts does not pose major privacy or information security issues. However, it is imperative to ensure ongoing compliance with all relevant legislations, including those governing FIPPA & CASL, as well as the UBC Information Security Standards and applicable UBC retention schedules.

6.3 Conditions of Approval

In the event of a significant change to the Art Mailing List platform (Sympa) or its usage by the Faculty of Arts, an amendment to the existing PIA will be necessary. Examples of significant changes include but are not limited to:

- Change in operational use and/or system access.
- Change in attributes accessed and used to create mailing lists.
- Integration with a new UBC software/system.

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
Daniel Pugh

Distribution
Requestor: Zoe Zhou, Project Administrator **Project Manager**: Julie Syenave, Project Manager **Owner**: Daniel Pugh, Associate Director, Service Strategy & Design **Risk Advisor**: Taylor Bohn, Information Security Risk Advisor

PIA Request Submission	Report Completion
2023-02-23	2023-10-19