PIA Guidance: Mass Email Tools

Overview

This document provides Privacy Impact Assessment (PIA) guidance for the expected use of mass-send or bulk-send email tools by UBC units. It ensures compliance with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA), *Canada's Anti-Spam Legislation* (CASL), and UBC's Information Security Standards, clarifying when a PIA is required.

A mass email tool is a software application or online service designed to send emails to large groups of recipients simultaneously. These tools facilitate the management of email campaigns, can automate message sending, and allow for personalized messages to effectively reach a wider audience. Key features typically include email list administration, customizable templates, scheduling options, analytics, and compliance functions to meet anti-spam regulations.

Pre-approved Tools

PIAs have been conducted for the following mass email tools:

- *Cyberimpact*
- *Envoke*
- *UBC Sendy (USEND)*
- *Student Communications Tool*

Use of these tools can proceed without a PIA, if the project owner or manager has completed the PIA Checklist.

PIA Checklist

To determine whether a PIA for use of a mass email tool is required, complete the PIA Checklist: Mass Email Tools (see below) and take the recommended actions, as necessary.

Academic Research Use

While this guidance primarily addresses administrative use of mass email tools, it is important to note that research applications often require approval from the Research Ethics Board (REB), especially when external recipients are involved. Most research likely to utilize mass email tools would fall under this requirement.

It is also relevant to consider platforms like REDCap or Qualtrics, which, though primarily designed for data collection, include functionalities to manage mass email communications within research settings.

(continued)

Tips and Reminders

Avoid Creating 'Phishy' Emails

- Where possible, send emails from a UBC email address and include contact information clearly in the email footer.
- Ensure the language is professional and direct, avoiding overly sensational content. UBC IT provides guidance to help make emails look authentic.
- Avoid vague or ambiguous language that might lead recipients to suspect the email is not legitimate.
- Never ask for sensitive information like CWL IDs or passwords directly in the email.
- When sending emails internally, ensure the "CAUTION: Non-UBC Email" banner is removed. UBC IT has developed a form for support with this.

Do Not Embed Hyperlinks

- Avoid embedding direct hyperlinks in the email, especially shortened URLs that obscure the destination.
- Encourage recipients to manually enter the URL into their browser and provide clear instructions on how to navigate to the desired page. This reduces the risk of phishing attacks.

Check the Recipient and CC Lists for Unintended Disclosure

- Do not include other recipient email addresses in communications.
- When recipients do not have a UBC email address, double-check to ensure that all recipients are BCC'd so their names and email addresses will not be disclosed to others.

Limit Personal Information Collection and Retention

- Collect only the minimal necessary personal information required for the communication's purpose. For example, only name and email address for a newsletter subscription.
- Ensure all personal information is securely disposed once the need to retain it expires.

Grant Access to Data Sparingly

- Restrict access to personal information to only individuals within UBC who need it to perform their duties.
- Regularly review and update access permissions.

Ensure Compliance with *Canada's Anti-Spam Legislation* (CASL)

- Apply CASL best practices by obtaining consent and providing unsubscribe options to maintain transparency and respect for recipients, even for non-commercial communications.
- CASL applies when communicating with external parties via electronic messaging to promote or encourage a commercial activity (see Guidance and Information on Canada's Anti-Spam Legislation).

Maintain Clear Identification and Privacy Notification

- Clearly identify UBC as the sender in every email.
- When an email will request personal information, include the required privacy notification (explaining the legal authority to request the information, how UBC will use the information, and who can answer questions about the collection). For more details, refer to the Privacy Fact Sheet – Collecting Personal Information.

(continued)

PRIVACY MATTERS @ UBC

PIA Checklist: Mass Email Tools

This checklist is designed to help navigate compliance requirements related to the use of mass email tools, ensuring alignment with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA), *Canada's Anti-Spam Legislation* (CASL), and UBC's Information Security Standards. Each section will help determine whether a Privacy Impact Assessment (PIA) is necessary or if further consultation with the PrISM SRS team is required.

Instructions

Read and respond to each of the questions in the table below, which may involve consulting additional resources, completing a PIA, or further discussions with the PrISM SRS team.

If ***all*** responses are **No**, no further action is required and the mass email campaign may proceed. Save a copy of this checklist for future reference.

If ***any*** responses are **Yes**, follow the necessary actions outlined in the table. Save a copy of this checklist for future reference.

Section	Question	Yes /No	Action if "Yes"
Tool Selection	Will the email be sent using a tool for which a PIA has not been conducted? *Note: PIAs have been conducted for Cyberimpact, Envoke, UBC Sendy (USEND), and the Student Communications Tool.*		Consult UBC Information Security Standards U1 and U9. Submit a PIA Inquiry for assistance, if required.
Data Handling	Will the email request personal information from recipients?		Consult the PIA Guidance for Survey Tools. A PIA may be required based on this guidance. If collecting personal information without using a Survey Tool, consult the Privacy Fact Sheet – Collecting Personal Information, and submit a PIA Inquiry.
Data Linkage	If you are requesting personal information, will it be combined with data from other public bodies?		A PIA is required. Please Request a PIA.
CASL Compliance	Is this communication considered a Commercial Electronic Activity (CEM) under CASL (See Applying CASL to UBC Activities)?		Complete the CASL – Compliance Checklist. If unsure whether CASL applies, or unsure about meeting requirements in the *CASL – Compliance Checklist*, request advice from the Legal Counsel, Information and Privacy.

Contact Us

For questions about this guidance, the PIA process, or to initiate a PIA Inquiry, visit Privacy Matters.