



PIA Guidelines: Mass Email Tools

Overview

This document provides Privacy Impact Assessment (PIA) guidelines for expected use of UBC's most frequently used mass email tools, and explains how to ensure that these tools comply with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) requirements and UBC's *Information Security Standards*.

The following tools are covered by these guidelines:

- [Cyberimpact](#)
- [Envoke](#)
- [UBC Sendy](#)

These guidelines do not apply to the use of other third-party mass email tools (e.g. *Campaigner*, *MailChimp*, *SendGrid*, and non-UBC versions of *Sendy*). Many of these tools are not compliant with FIPPA because they store personal information (PI) outside Canada. A PIA request must be submitted if you are planning to use these or any other tools and will be collecting PI. For more information about how to submit a PIA request, refer to the [UBC PIA Webpage](#).

General Requirements

PIAs have been conducted for *Cyberimpact*, *Envoke*, and *UBC Sendy*. These tools can be used within the University community for most purposes. However, you may be required to submit a supplementary PIA request depending on a number of factors, such as the nature of PI collected, how such information is used, shared or disclosed, and where it will be stored. For information about what constitutes PI, refer to the Fact Sheet [What is Personal Information?](#)

Supplementary PIA Required

A supplementary PIA is required if **any** of the following factors apply:

- If you have not yet obtained consent or have authority under FIPPA to send targeted emails
- PI will be gathered for, or requested by, the mass email
- PI will be accessed by, disclosed to, or obtained from another unit within UBC
- A third party external to UBC (other than *Cyberimpact*, *Envoke* or *UBC Sendy*) is involved in the project
- PI will be used for marketing or promotional purposes, or disclosed to the general public
- PI will be used for purposes other than the original purpose that are not expressly stated in the mass email
- Mass email data will be linked to other PI without the data subject's consent

Supplementary PIA Not Required

If none of the above factors are applicable, then you are not required to request a supplementary PIA.

A supplementary PIA is also not required if your use of these tools is part of a research project that has received Research Ethics Board approval, or if you are using these tools as a student for academic purposes. However, you should still follow the Tips and Reminders below.

(continued)

Tips and Reminders

Administrators should always adhere to the following principles when creating mass emails and managing data collected using these tools:

- **Obtain approval to use mailing lists:** If the list of email recipients was obtained from UBC, appropriate approval for use of the list must be obtained from the data custodian.
- **Comply with CASL:** Although not directly addressed by this guideline, all mass emails must comply with the [Canada's Anti-Spam Legislation](#).
- **Avoid creating 'phishy' emails:** Never ask people to provide their CWL ID or password. A common way for hackers to gain personal information is through fake survey invitations that ask for login credentials. UBC IT has developed [guidelines](#) to help you make your emails look authentic.
- **Avoid embedding links:** Do not include links that require people to click on them; direct people to navigate to the required site on their browser.
- **Limit PI collection and retention:** PI and user metadata collected by mass emails (e.g. via tracking links for analytics purposes) should be guarded closely and purged when the mass email is completed.
- **Grant access to data sparingly:** Mass email creators and data custodians are responsible for ensuring that access to data containing PI is granted on a "need-to-know" basis with third parties to limit unintentional PI disclosure.
- **Offer an opt-out:** regularly distributed emails or newsletters are required to have an opt-out feature for recipients.
- **Don't disclose PI:** Do not make PI available to the general public.
- **Consider a privacy notification (if required):** Under FIPPA, you must provide a privacy notification anytime PI is collected or used. As long as the individual sees the notification, it is not necessary for them to click "I agree".

Contact Us

For questions about the information contained in these guidelines or the PIA process, contact pia.process@ubc.ca.