Privacy Impact Assessment for:

VANCOUVER ISLAND UNIVERSITY

Constant Contact

Initiative Name	Constant Contact Email platform
Department Name:	External Relations

VANCOUVER ISLAND UNIVERSITY

Constant Contact

Part 1 – General Information and Overview

1.1 What is the Initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

Constant Contact is a web-based email marketing software (Software as a Service) that primarily helps businesses create branded emails, landing pages, and more in one online marketing platform. VIU will use this platform for all email marketing and student, alumni and community engagement including newsletters, event invitations and announcements. Names and email addresses are stored on the platform. Subscribers are sorted into lists of their choosing and/or segmented by their VIU affiliation. Professional/workplace contact information for invitations or targeted communications are uploaded from contacts provided by student services and human resources and maintained in specifically labeled, limited-use distribution lists. Constant Contact does not sell or rent email addresses. Users are not permitted to upload or use purchased, traded, shared, or borrowed lists to their Constant Contact account. Similarly, VIU does not sell or share its email lists from Constant Contact. All contact management and email communication are done in compliance with CASL.

1.2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

Constant Contact will be used by VIU for the following:

Email marketing
- sending promotional messages for recruitment purposes
- event promotion
- prospect newsletters

Community engagement
- distribution of digital newsletters to students, staff/faculty and alumni
- periodic communication with donors
- event invitations and sign-up

Reporting and analytics
- The Constant Contact platform has reporting features that allow VIU to monitor email campaigns for impact and effectiveness. Email campaigns sent from Constant Contact includes a web beacon that allows it to determine, on behalf of their customers, if an email is opened, as well as the email delivery status and geographic location. Email campaigns may also contain other tracking technology

that allows them to determine what is clicked on in an email and if someone unsubscribes or changes their subscription preferences. This web beacon and other tracking technologies also allow Constant Contact to collect log data, including a user's IP address, browser type and version. Constant Contact shares information about email delivery, email opens, email clicks, and subscription preferences with its customers so they can optimize their campaigns, customize offerings, and understand subscribers' level of engagement with them.

This PIA covers Constant Contact only - not the systems that may be used to provide contact data for importing (SalesForce, Raiser's Edge, SRS).

1.3. Are there any related Privacy Impact Assessments?

Please indicate if this an update on an existing PIA or an additional module that was not covered in the original PIA.

N/A

1.4. What are the data or information elements involved in your initiative?

In the table below, please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in an appendix.

Information Type	Information Collected
Personal Information	**Students and Community members**: First name Last name Email address **Students, employees, community members**: IP address **From Prospective Students:** Country of citizenship; IP address **From Alumni:** VIU education credentials; IP address
Contact details	VIU Employment contact info: First name Last name Email address

Account information: what info is required to set up an account?	N/A
Commercial information	N/A

1.4a. Did you list personal information in question 1.4?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference- see the table below for examples of Personal Information.

Business contact information, in turn, is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, as well as business telephone number, address, email or fax number of the individual. BC FIPPA does not protect business contact information.

Examples of Personal Information	
• Name, age, sex, weight, height • Home address, phone number • Race, ethnic origin, sexual orientation • Medical information • Health history • Number or symbol assigned to the individual • Income, purchases and spending habits • Blood type, DNA code, fingerprints	• Marital or family status • Religion • Education • Financial information • Criminal information • Employment information • Personal views or opinions, except if they are about someone else

- If yes, go to Part 2
- If no, answer question 1.5 and submit questions 1 to 1.5 to pia@viu.ca. You do not need to complete the rest of the PIA template.

Yes

1.5. How will you reduce the risk of unintentionally collecting or disclosing personal information?

Some initiatives that do not require personal information are at risk of collecting, using, or disclosing personal information inadvertently, which could result in an information incident.

N/A

Part 2 – Collection, Use, and Disclosure

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

2.1 Four point "Necessity Test" for the collection, use, and disclosure of Personal Information.

To determine if the Personal Information from your initiative meets the necessity threshold, apply the following four-point test to each element of PI from 1.4 above. Note that each element of PI must meet all four points of the test.

Four point "necessity test" for collecting personal information (OIPC Canada, 2016).

1. The information is rationally connected and demonstrably necessary to an operating program or activity
2. The information is likely to be effective in meeting the objectives of the program or activity
3. There are no other less privacy-invasive ways to effectively achieve the objectives of the program or activity
4. The loss of privacy is proportional to the objectives of the program or activity

Personal Information element	**Does it meet all four points of the necessity threshold?**	**Reasons for keeping or excluding from initiative**
First name	Yes	Necessary for personalizing communications
Last name	Yes	Necessary for personalizing communications
Email address	Yes	Necessary for the use of the tool
Country of citizenship	Yes	Necessary to ensure accurate information is shared with prospects
VIU education credential	Yes	Necessary to ensure relevant information is shared with alumni
Web beacons: record each contact's email address, IP	No	Open rates, click rates, date, and time are shared back with VIU for email campaign purposes (optimize email marketing campaigns,

address, geolocation, date, and time associated with each open and click for an email campaign		customize offerings, and understand subscribers' level of engagement with them). Subscription preferences are tracked for unsubscribe options. It is not clear why IP addresses and geolocation are tracked.

2.2 Does your initiative involve the use of Artificial Intelligence (AI)? If so, please fill out Appendix One: GenAI Analysis Questions

N/A

2.3 Personal Information Flow Diagram and/or Personal Information Flow Table

In the table below, list the personal information from question 1.4. Think about how each element of information flows through your project. Your Privacy Officer can help you figure out whether each step is a collection, use, or disclosure, and whether you have the legal authority for the way you're working with the information. Alternatively, you can attach a flow diagram to this PIA. Add rows as necessary.

	Describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**(Collection, Use or Disclosure)**	**FIPPA or other legal authority**
E.g.	*E.g., Student email, password, and IP address collected by software platform for account creation.*	*Collection*	*FIPPA 26(c) "info relates to and is necessary for a program or activity"*
1.	A user submits their name and email address via online sign-up form to request program information, event updates and other VIU news. The user "opts in" to email marketing and consent is explicit.	Collection	FIPPA s. 26(c)

2.	Information provided by internal partners: Contact lists are supplied by internal departments to manage internal business communications. Lists come from the Student Records System (current students), human resources (employees) and Raiser's Edge (alumni) and are manually uploaded to Constant Contact.	Disclosure (to Constant Contact servers)	s.33(2)(d)
3.	Prospective student lists are integrated with Sales Force CRM to allow recruiters to better manage leads.	Collection, Use, Disclosure	s. 26(c); s.32(a); s. 33(2)(d)
4.	Email communications are sent to users based on their selected preferences and/or VIU affiliation Opt-out mechanisms are provided in every email.	Use	s.32(a)
5.	Web beacons record each contact's email address, IP address, date, and time associated with each open and click for an email campaign. Information about email delivery, email opens, email clicks, and subscription preferences, as well as aggregated information about browser types is shared back to VIU	Collection by CC from VIU member; Disclosure CC to VIU; Use by VIU (metrics);	s. 26(c); s.33(2)(d); s. 32(a);
6.	Event sign up: VIU Employee, student, community member registers for an event held by VIU Info collected on form: First name, Last name, Email, Yes I am attending, No I am not, Any dietary restrictions (long form), Any additional information events staff require (such as accessibility needs).	Collection by VIU; Use by VIU; Disclosure to CC	s. 26(c); s. 32(a); s.33(2)(d)

2.4 Risk Mitigation Table

Thinking through the information flow, identify where there are risks for privacy incidents or data breaches. For each risk, identify a mitigation strategy, as well as the likelihood of an incident, and level of impact or harm if people's information were breached.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact/harm**
1	Unauthorized access	VIU employee access is granted through role-based access control permissions (RBAC). Only top-level access roles can export contacts. Additionally, sub-accounts within Constant Contact ensure users only have access to the contacts related to their communication needs. For RBAC details, see 5.3.1 below.	Low	Low
2	Data breach/loss	Incident Management Constant Contact has a documented Cybersecurity Incident Response Plan and 24x7 security monitoring. The Cybersecurity Incident Response Plan undergoes annual tabletop testing and is updated as necessary. Constant Contact Information Security Program **Vulnerability Disclosure Program** At Constant Contact the safety, privacy, and security of the data our customers entrust to us is very important to us. We welcome the	Low	Med

		reporting of security vulnerabilities in our product and services and encourage researchers to reach out to us when they find issues. To assist that greater good, Constant Contact encourages security researchers, ethical hackers and our users to report security flaws that they may discover through our Security Vulnerability Responsible Disclosure Policy.		
3	Users are not comfortable/do not want to be tracked by web beacons and cookies embedded in emails.	According to Constant Contact's "Customer Contact Data Notice" a link to which is provided in the footer of all emails sent through the platform: "Web beacons may be refused when delivered via email by disabling HTML images or refusing HTML (select "Text Only") emails via your email software. Other tracking technologies used in VIU/Constant Contact email campaigns are only activated when you click on a link in an email or otherwise interact with content in an email, and you may opt out of such data collection by not interacting with emails sent from the platform." The VIU Privacy Office is developing a detailed guide about Web Beacons, Cookies, and other tracking technologies, with suggestions for how to prevent or avoid being tracked. This guide will be published	High	low

		on the VIU Access & Privacy website and linked to from Privacy Notifications through out the VIU websites.		
4	Tracking (persistent) Cookies: Constant Contact or another third party may set a cookie on a user's browser when accessing an event registration form, donation form, or similar website from a customer's email in order to better track visitors to such a website.	Learn how to disable/block third party cookies on your web browser: https://allaboutcookies.org/cookie-profiling Consider using VPN Switch to a privacy-first browser such as Duck Duck Go	High	low
5				

2.5. Collection or Privacy Notice

If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice, also known as a privacy notification.

A collection notice must contain the following elements:

- The legal authority and section under FIPPA under which you are collecting personal information.
- The purpose for which you are collecting the personal information and how it will be used.
- The contact information of an employee or officer at VIU who can answer questions about the collection of personal information.

Contact the privacy office for a collection/privacy notice template.

https://gov.viu.ca/access-and-privacy-viu https://www.constantcontact.com/legal/privacy-notice

Constant Contact

VIU Marketing has confirmed that there are privacy notifications in place at all personal information collection points on the VIU website relevant to this initiative (where collecting contact information will be used for marketing and information emails).

Part 3: Storing Personal Information

3.1. Is any personal information being stored outside of Canada?

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

All data is stored outside of Canada using both OnPrem and Cloud storage in the US. The data is not sensitive in nature.

3.1.1. Where is the personal information stored?

On Constant Contact servers in the US.

3.2. Does your initiative involve sensitive personal information?

Examples of sensitive personal information include personal health information, genetic and biometric data, personal finances, geolocation data, criminal records, counselling records, HR records, payroll records, racial or ethnic origin, sexual orientation, religious, philosophical, or political beliefs, etc.

N/A

If **yes**, please complete **Part 4**: Assessment for Disclosures of Sensitive Personal Information.

If **no**, skip to **Part 5**: Security of Personal Information

Part 4: Assessment for Disclosures of Sensitive Personal Information

Complete this section if you are disclosing sensitive personal information. You may need help from your organization's Privacy Officer.

4.1. Is the sensitive personal information stored by a service provider?

N/A

If yes, fill out the table below, then go to question 4.3. If no, continue to question 5.

Information about Service Provider

Name of service provider	**Name of cloud infrastructure and/or platform provider(s)**	**Where is the sensitive personal information stored (including backups)?**
N/A		

4.2. Provide details on the disclosure, including where and how the personal information is stored.

Answer this if question 4.1 does not apply. Be specific about where and how the information is being stored.

N/A

4.3. Is there a contract that includes privacy-related terms?

If there is a contract with the provider, please describe any privacy-related terms in the contract, or attach the privacy schedule.

N/A

Part 5: Security of Personal Information

Section 30 of FIPPA imposes a duty on the public body to prevent unauthorized access to Personal Information both internally and with any contracted third parties. As such, we need to make sure that personal information is safely secured in both physical and technical environments. **For each item in this section, please describe the security measures for both the service provider and for VIU internally.**

5.1. Please describe the physical security measures related to the initiative (if applicable).

For example, physical security measures may include: the security environment of vendor's data centres; storing records containing PI in locked storage rooms, offices, and/or filing cabinets with controls over distributions of keys/access; locked workstations that do not permit others to view your screen (including when working remotely, etc.

Physical access to Constant Contact's hosting environment is restricted to specific individuals and uses multiple levels of security as follows:

Constant Contact servers and infrastructure are located in secure data centers where access is limited to authorized personnel and badge access or biometric authentication (e.g., hand scanners and fingerprint IDs) are required to access the facilities.

Constant Contact servers are isolated and secured within the data center in areas dedicated to Constant Contact equipment only; these areas are not shared with third parties.

Access to data centers and hosting systems are regularly reviewed by Constant Contact's data center operations team to assure that only authorized users have access.

7×24 security guards perform random checks of the data center to ensure physical security controls have not been compromised.

5.2. Please describe the technical security measures related to the initiative (if applicable).

E.g. Encryption standard for data in transit and data at rest; firewalls, strong passwords; MFA; encrypted documents, etc.

Network Security

Constant Contact requires that network communications adhere to the principles of data confidentiality, integrity, and availability discussed above.

Constant Contact's hosting environment is protected from the public Internet and corporate Local Area Network (LAN) via multiple next-generation firewalls and is monitored by an intrusion prevention/detection system, including a strategically placed distributed denial of service mitigation system.

Constant Contact requires that information is handled with appropriate levels of encryption in accordance with our policies and standards and to comply with applicable laws.

Customer Hosted Environment Security

Constant Contact performs industry-standard security hardening efforts -- more specifically, critical

systems are hardened and configured per industry best practices as defined by the Center for Internet Security (CIS).

Constant Contact regularly reviews information on current security vulnerabilities, including vendor announcements and other industry sources. If security updates are determined to be critical to the Constant Contact environment, they are tested and deployed in a timely manner.

Customer hosting systems and services are routinely monitored for integrity and availability. Operations staff review alerts generated by monitoring systems and respond promptly.

Customer hosting systems are monitored 24×7 for malicious activity.

Administrative access to Constant Contact's infrastructure is limited strictly to authorized users with multi-factor authentication. Individual usernames and passwords are required for machine and data access.

Constant Contact adheres to strong password guidelines, including complexity and minimum length requirements. Passwords are expired and changed on a regular basis.

Development Security

Internally developed code is subject to Constant Contact's secure coding guidelines, which includes testing of functionality and business logic, and for security flaws. In addition, our Change Management Policy ensures that code deployed to the production environment has been appropriately tested, reviewed, and approved.

We train our engineers in secure coding and architectural design patterns such as those outlined in the OWASP Top 10, CIS Critical Security Controls, and NIST frameworks.

As part of Constant Contact's ongoing PCI compliance, we regularly undergo security reviews, including external and internal scanning for vulnerabilities on an ongoing basis. All vulnerabilities discovered are reviewed by internal security and addressed in accordance with the level of severity.

User Account Security

User-level access to Constant Contact services is provided via a username and password selected by the end user. Constant Contact enforces strong passwords and also offers Multi Factor Authentication (MFA) to its customers, which is strongly recommended for the security of your data.

Passwords and credit card numbers are encrypted.

Constant Contact

User account setup, maintenance, and termination are under the control of the end user.

Incident Management

Constant Contact has a documented Cybersecurity Incident Response Plan and 24x7 security monitoring.

The Cybersecurity Incident Response Plan undergoes annual tabletop testing and is updated as necessary.

Personnel Security

Constant Contact employment offers are contingent upon successful completion of a criminal background and reference checks where allowed by law.

Upon commencing employment, all Constant Contact employees receive information security training and are contractually obligated to confidentiality clauses to ensure that they adhere to Constant Contact's commitment to security and confidentiality.

Constant Contact's information security awareness and training programs require employees to complete annual security refresher training.

Patch Management

Where feasible, system components and software are protected from known vulnerabilities by applying the latest vendor-supplied security patches.

Constant Contact systems are routinely updated per vendor recommendations and industry standards.

Virus/Malware Management

Constant Contact uses up to date virus scanning software for detecting currently known malware.

Malware definitions are updated daily and installed as required.

Operations teams monitor the Constant Contact hosting environment 24×7 for malware infections.

5.3 Tracking Access / Access Controls. In this section, you will describe how the unit will minimize the risk of unauthorized access to Personal Information.

5.3.1. FIPPA section 30 requires public bodies to manage access to PI based on the principle of "need to know" – that users may only access information that is necessary to do their job. This is frequently accomplished by assigning role-based access controls (RBAC), and by establishing a security matrix that describes which positions/roles are permitted to access specific types or groups of Personal Information. Access to personal information should only be permitted to those who demonstrate their right of access on the security access chart. Please describe how access controls work in the department, or with this initiative.

Account Owner: Account owners can access all resources and operations that are currently available in the V3 API., contacts: read, write; contacts-lists: read, write; ui-campaign: metrics; campaign: read, create, write, send; account: read, update

Account Manager: Account managers can access all resources and operations that are currently available in the V3 API., contacts: read, write; contacts-lists: read, write; ui-campaign: metrics; campaign: read, create, write, send; account: read

Campaign Creator: Campaign creators are limited to creating campaigns, updating campaigns, viewing campaigns, and viewing contact lists. Campaign creators cannot send campaigns, access contacts, view reports, or modify contact lists., campaign: read, create, write; contacts-lists: read

Account Owner and Account Manager Differences: Account owners can use the Constant Contact UI to add users, modify user roles, and change billing information. Account managers cannot add users, modify user roles, or change billing information.

Most VIU users will have **Campaign Creator roles**. Each sub-account is limited to one Account Manager. Marcomm will assign two Account Owners for redundancy.

5.3.2 How will you know if sensitive personal information is accessed, including access by service providers? This should include a description of what information is available through logs.

N/A (no sensitive info collected in this initiative)

5.3.3 Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

See 5.3.1 above for Role-based Access Controls

5.4 What controls does the provider have in place to prevent unauthorized access to sensitive personal information?

Describe technical, administrative, and/or policy measures in place to protect PI. If using a cloud-based service provider, include a description of controls in each layer of the stack: software level, platform level, infrastructure level.

N/A – no sensitive PI collected in this initiative.

Part 6: Accuracy/Correction/Retention of Personal Information

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete. In this section, you will demonstrate how you intend to keep personal information on file accurate and complete.

6.1 How is an individual's information updated or corrected?

FIPPA section 29 states that a person can ask you to correct their personal information in your custody or control. If it is not possible to update or correct (for physical, procedural or other reasons) it must be noted on the record. **Please explain how it will be updated or annotated. If personal information will be disclosed to others, how will VIU notify them of the update, correction, or annotation?**

All emails sent through the Constant Contact platform include an easy, automated way to stop receiving marketing emails from the sender (unsubscribe). Users can also change the topics they're interested in by updating their profile. If a users wishes to unsubscribe or update their profile, they simply click on the Unsubscribe, SafeUnsubscribe® and/or Update Profile links at the end of any email received.

6.2. Does your initiative use personal information to make decisions that directly affect an individual(s?

N/A

6.2.1.If you answered "yes" to question 6.2, do you have an information schedule in place related to personal information used to make a decision?

FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

N/A

6.3. Do you have a records management schedule in place?

How long will you keep the personal information collected? Is there a plan in place for retention and deletion? Please also use this question to note how long it will be stored by the service provider (if applicable).

Internal lists are regularly updated to add/remove contacts whose business relationship with VIU starts or ends Contacts who have opted in to email communications remain in the list indefinitely until they elect to unsubscribe. Approximately once a year, unengaged contacts (those who have not opened an email in more than six months) are archived from active lists.

Part 7 – Personal Information Banks

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

7.1. Will your initiative result in a personal information bank?

Yes

If yes, please complete the table below:

VANCOUVER ISLAND UNIVERSITY

Constant Contact

Describe the type of information in the bank
First name, last name, email address for employees, students, and alumni First name, last name, email address, citizenship for prospective students
Name of main organization involved
VIU
Any other ministries, agencies, public bodies or organizations involved
Constant Contact
Business contact title and phone number for person responsible for managing the Personal Information Bank
Allie Voisin, VIU Director, Strategic Communications, allie.voisin@viu.ca

Part 8 – Further Information

8.1. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

N/A

8.2. Will the information collected be used for research or statistical purposes?

N/A

Part 9 – Summary and Proponent Responsibility

This section is for Privacy Office recommendations as well as any limitations due to privacy concerns.

I have reviewed the data security practices of the service provider, and I am satisfied there are reasonable security arrangements with respect to s. 30 of the BC FIPPA. With regard to privacy, the personal information collected is limited and non-sensitive and the vendor's privacy safeguards meet industry standards with respect to protecting personal information.

Constant Contact

The main privacy concern is with the use of web beacons that Constant Contact embeds in the body of emails. Web beacons are a tracking and surveillance technology that collect meta data such as IP addresses, geolocation, and engagement information such as email opens and click rates. The presence of web beacons in emails are hidden so users are likely unaware that their metadata is being collected. Further, IP addresses were recently considered personal information by the Supreme Court of Canada, which means public bodies need to start treating this type of data as personal information- such as including in privacy notifications.

As stated above, the footer of all VIU email communications sent on the platform contain a link to the provider's "Customer Contact Data Notice," and within that notice, there is a description of how web beacons are used as well instructions for refusing web beacons and avoiding other embedded tracking technologies.

In addition, the VIU Privacy Office is developing a detailed guide about web beacons, cookies, and other tracking technologies, with further suggestions for how to prevent or avoid being tracked. This guide will be published on the VIU Access & Privacy website and linked to from Privacy Notifications throughout the information collection points across VIU websites.

Part 10: Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Reviewed by	Privacy Officer
Approved by	Director, Strategic Communications
Date:	2025-04-17