Privacy Impact Assessment for:

Behaviour Intervention Team (BIT): Maxient Integration

Initiative Name:	Behaviour Intervention Team (BIT): Maxient Integration
Department or Service Area	Student Affairs: Student Conduct and Care

Privacy Impact Assessment for:

Behaviour Intervention Team (BIT): Maxient Integration

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.

The Vancouver Island University (VIU) BIT Team is a multi-disciplinary group dedicated to identifying and supporting students who may be experiencing distress, exhibiting concerning behaviour, or facing barriers that impact their wellbeing or academic success. The initiative outlined in this assessment involves using Maxient, a secure, cloud-based case management system, to streamline, document, and coordinate BIT Team efforts.

The purpose of this initiative is to enable efficient, confidential, and collaborative tracking of student care-related concerns and interventions. The system allows for centralized documentation of referrals, outreach attempts, follow-ups, case notes, and support plans, with appropriate access controls to ensure only authorized personnel can view sensitive information.

By adopting Maxient, the BIT can improve consistency, minimize information silos, and support early intervention through timely communication and action. The system also helps in facilitating proactive, trauma-informed responses while maintaining compliance with privacy legislation and institutional policies.

The BIT Team initiative includes partnerships and coordination with multiple stakeholders across the institution, including Student Affairs service teams, Student Health and Wellness, DEHR, Student Housing, Security, and Indigenous and International student supports. Staff from these areas may serve as referrers, collaborators, or contributors depending on the situation and student needs. The Student Conduct and Care Office is the lead unit responsible for system administration and oversight of the Maxient platform.

The initiative is ongoing, with Maxient serving as the current system of record for Student Conduct and Care related files (Resource Request and Referrals - formerly Early Alert, Student Conduct, etc). This ensures that historical context and evolving needs can be appropriately understood and responded to, even across academic terms or years.

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?

This PIA specifically covers the expansion of Maxient case management access to include the VIU BIT Team, enabling them to securely document, coordinate, and track student support cases within the platform. It includes configuring access-controlled user accounts for BIT Team members, defining

role-based permissions, and migrating active and historical case tracking processes from shared Microsoft Teams spreadsheets into Maxient. All historical case information will be deleted from M365 after migration to Maxient.
The scope of this PIA is limited to the use of Maxient by the BIT Team for non-disciplinary student support and wellbeing case management. It includes documenting referrals, case notes, risk or concern indicators, and follow-up actions relevant to the BIT Team's work. This expansion supports increased consistency, confidentiality, and collaboration within existing institutional protocols for student support.
Out of scope for this PIA is the broader use of Maxient by other departments (e.g., Student Conduct and Care, Security, and DEHR), which are covered under previous privacy assessments and operational procedures. Additionally, this PIA does not cover any new data collection methods, changes to referral sources, or the integration of third-party systems or tools with Maxient.

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.

This is an update on the existing PIA related to Maxient.

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	**From Students:** Resource, Request and Referral form submitted by employee: name, phone number, email, campus of form submitter; name and student number of student (if known); type of concern; course name; contextual details of concern; supporting documents (photos; screenshots of communications; meeting notes, etc.) Resource, Request and Referral form submitted by student or friend of student in distress: Name, phone number, email, campus of submitter; name phone no., email of student of concern; type and details of concern; supporting documents (photos, screenshots of communication, etc.). Other: response plans created by BIT team; communications about student of concern; case notes; risk of concern indicators; follow-up actions; **From Third Parties:** **From VIU Employees:**

Contact details	**From Students:** **From Third Parties:** **From VIU Employees: name, contact phone number and email address**
Account information: what info is required to set up an account?	
Commercial information	

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.

Click or tap here to enter text.

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
Resource, Request and Referral form:		
Contact info of form submitter (name, phone, email, campus)	yes	This information is necessary to validate the source of the concern, enable follow-up for clarification, and ensure accountability. Anonymous reports limit the ability to triage effectively. The collection is proportionate and essential for reliable assessment and coordination.
Student name	yes	Identifying the student is foundational to addressing concerns, ensuring accurate case management, and avoiding confusion with others. It is a

		minimal privacy impact in relation to the necessity of targeted intervention and support.
Student number (if known)	yes	Student numbers help confirm identity, especially where multiple students share similar names. While not always required, this detail improves accuracy in accessing records and providing coordinated care.
Type of concern and contextual details	yes	Detailed descriptions are essential for assessing the nature and severity of the concern. Without context, BIT cannot make informed decisions or prioritize appropriately. The information collected is directly tied to the intervention's effectiveness.
Supporting documents: photos, screenshots of communications; meeting notes, etc.	yes	Supporting evidence strengthens the credibility and accuracy of referrals. These documents allow BIT to evaluate behaviour or risks more objectively. Collection is limited to relevant materials.
Other:		
response plans created by BIT team	yes	Response plans are necessary for documenting coordinated actions, accountability, and follow-up strategies. They are fundamental to delivering support and managing risk effectively.
communications about student of concern;	yes	Ongoing internal communications ensure informed, consistent responses across departments and service areas. This supports transparency and continuity in care.
case notes	yes	Case notes document observations, decisions, and actions taken. They are essential for accountability, ongoing assessment, and risk management within the BIT process.
risk of concern indicators;	yes	These indicators are used to assess behavioural patterns and risk levels. Collecting and tracking them enables consistent, evidence-based triage and intervention.
follow-up actions;	yes	Documenting follow-up ensures that supports are delivered and that the student's situation continues to be monitored. It allows for timely reassessment and closure of cases when appropriate.

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.	Information related to students who are struggling (academic, mental health, financial, housing etc.) will flow directly into Maxient via our online Resource Request and Referral forms. https://cm.maxient.com/reporting.php?VancouverIsland	Collection/Disclosure (to Maxient)	Collection: s. 26(c); Disclosure: s.33(2)(d)
2.	The Conduct and Care team have access to submitted forms – their role is to triage the request and determine the appropriate level of response. Responses: • Typical/Low Level or Singular Concern Noted: Forward the request directly to appropriate service area via secure	Use/Disclosure	Use: s. 32(a) Disclosure: s. 33(2)(c) with consent/self-disclosure; s. 33(2)(d)

	Maxient link, for outreach to student (Counselling, Advising, etc. - this has been the historical practice for all requests and former Early Alerts) • Multiple Concerns Noted or Mid/High Level Concern: Alert appropriate BIT team members to gather more information and develop response plans. This would include adding BIT members to a shared case file in Maxient until the case is concluded. All information gathered would remain in the Maxient file and case members would be removed after the case is closed.		

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	Employee added to file – not involved etc.	Create SOP for determining and adding appropriate CARE/BIT members to files	Low	Student information shared with inappropriate person – could increase risk of bias
2	Employees have access to sensitive information while working on the file	Privacy (Records Mgmt) courses – have the Privacy Office confirm individuals have taken course PRIOR to adding them to Maxient/BIT team.	Low	Potential for bias or use of information outside of intended purpose

		Terms of Reference to include specific confidentiality/privacy expectations of BIT members Access to files is tracked via activity log – Manager of Conduct will review activity log regularly		
3.	Inadvertent breach: E.g. Employee downloads file with sensitive information and shares with unauthorized person, or stores in location that can be accessed by unauthorized individuals.	Mandatory VIU Privacy and Records Management courses Terms of Reference to include specific confidentiality/privacy expectations of BIT members	Med	Student privacy breach /FIPPA violation.
4.	Conduct and Care triages and sends RRR form to wrong individual	Mandatory VIU Privacy and Records Management courses Prevention measures such as providing access to documents rather than sending email attachments.	Med	Student privacy breach /FIPPA violation.
5.	Sensitive information is breached in transit to Maxient or from Maxient servers.	See Maxient PIA for all security measures	Low	Severe

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.

The personal information collected through this form is collected under the authority of the *University Act* and is protected under the *Freedom of Information and Protection of Privacy Act (FIPPA)*. This information will be used to help coordinate appropriate support for students by sharing relevant details with the VIU departments best positioned to help—such as Advising, Counselling, Accessibility Services, Student Housing, and other support areas directly involved in student well-being and success.

In some cases, limited information may also be shared on a need-to-know basis with members of VIU's Behaviour Intervention Team (BIT) or Threat Risk Assessment Team, if there are concerns about safety, significant risk, or overall well-being.

Information submitted through this form will be used only for the purposes of student support and risk assessment, as described above. It will not be used or disclosed for any other purpose unless authorized or required by law.

If you have questions about the collection, use, or disclosure of personal information, please contact VIU's Privacy Office at Privacy.Officer@viu.ca.

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.

See Maxient PIA

3.1.1. Where is the personal information stored?

See Maxient PIAClick or tap here to enter text.

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.

Yes

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?

See Maxient PIA

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)?**

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.

See Maxient PIA

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.

See Maxient PIA/Contract

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.

See Maxient PIA

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.

See Maxient PIA

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.

See Maxient PIA

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.

System logs

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.

Each CARE user will be assigned a specific access level, which does not allow them to change personal info. Access is tracked via system log, the Manager of Conduct and Care will review access logs regularly, as well as do random checks.

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.

Systems levels - each user will only be able to access files they are assigned to and will have specific security level. Once a case has concluded, the Manager of Conduct and Care will remove the collaborating CARE/BIT team members from the case file.

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?**

SRS feed is automatically updated daily. A level 5 user can also update/correct information – we will review and refer to VIUs Correction of Personal Information Best Practices Guide to ensure compliance. Only the Manager of Student Conduct and Care currently has level 5 access for student cases.

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

Yes

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.

Records management update and institutional records retention schedule coming – we will comply with that.

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).

Currently we retain general student conduct files for 5 years and high risk (violence etc) indefinitely after most current registration. We will be reviewing the records retention schedule and expectations, and can arrange to have Maxient set up a scheduled purge of outdated files.

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?

No

If yes, please complete the table below:

Describe the type of information in the bank
Name of main organization involved

Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

Part 8 – Further Information

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

Click or tap here to enter text.

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

The Student Conduct and Care team compiles an annual report which notes the case types (conduct, CARE etc) but does not include any personal information.

Part 9 – Summary and Proponent Responsibility

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

- Manage records within Maxient when possible, to avoid downloading (duplicating) and storing in multiple locations.
- During BIT meetings, assign single notetaker (so multiple notes are not generated) and ensure notes are stored in student's Maxient file only.
- Proponent has committed to creating Role-based Access Control (RBAC) document/SOP that lists access levels of various roles/positions as well as adding and removing individuals.

- Proponent has committed to ensuring all CARE/BIT team members will take both the VIU Access/Privacy and Records Management courses prior to getting access to Maxient/ case files.
- Proponent has committed to creating Terms of Reference to include specific confidentiality/privacy expectations of CARE/BIT members.
- Revisit/update PIA in one year to include established retention periods for records.

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.

Role	**Name**	**Electronic signature**	**Date**
Initiative lead	Manager, Student Conduct & Care		2025-09-11
Program/Department Manager (if different from initiative lead)			