# Privacy Impact Assessment
# Emily Carr University of Art + Design
## *Anonymous Reporting Tool*
PIA# *2024-##*

## Part 1 – General Information

| | | | |
|---|---|---|---|
| **Name of Department/Unit** | Student Services | **Project ID** | N/A |
| **PIA Drafter** | Kaitlyn Gutteridge / Justine Langille | | |
| **Email** | kgutteridge@ecuad.ca / justinlangille@ecuad.ca | **Phone** | 778-833-0628 (Kaitlyn Gutteridge) |
| **Project Sponsor** | Sue Dorey | | |
| **Email** | Sdorey@eduad.ca | **Phone** | 604-844-3819 (Sue Dorey) |
| **Project Manager** | Sue Dorey; Justine Langille | | |
| **Email** | sdorey@ecuad.ca; justinlangille@ecuad.ca | **Phone** | 604-844-3819 (Sue Dorey) |

### 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.*

As part of Emily Carr University's (ECU) alignment with the B.C. Government's *Sexual Violence and Misconduct Policy Act, Sexual Violence and Misconduct Policy Act* and the concurrent Post-Secondary Sexualized Violence Action Plan (2022), which sets out imperatives to respond to and prevent sexualized violence at British Columbia Post-Secondary Institutions, ECU is developing and launching an anonymous reporting tool.

The Anonymous Reporting Tool (ART) is an electronic form that will be made available on the ECU website that enables students to anonymously report/share information on sex and gender-based violence and other forms of misconduct experienced under ECU jurisdiction[1].

With the announcement by the B.C. Government outlining requirements to make an anonymous reporting tool available at ECU, ECU undertook an assessment of various third-party reporting tools (i.e., privacy and security controls, feasibility, user experience) over the 2023-2024 academic year. It was determined that GlobaLeaks, a free and open-source whistleblowing software that enables the

[1] Jurisdiction as defined in ECUAD's Policy 3.6 Sexual and Gender-Based Violence and Misconduct Policy

creation of secure whistleblowing projects, would be used as the foundational platform for developing and launching ART. At the time of drafting, ECU IT was finalizing steps to tailor the software to meet requirements needed to create a secure and anonymous tool for submitting reports of sexualized violence. ART will be released in August 2024 to align with the start of the 2024-2025 academic year.

ART permits an individual to submit a report without providing any personal information. To do so, the individual is provided with access to a secure link to ART via ECU's website – no username or password is required to login to the form's site. Once directed to the form's website, the individual is provided with ECU's collection notice (as per FIPPA requirements) along with an overview of requirements for using the form and submitting a report. Once the individual is ready, they respond to the questions in the form; both structured and unstructured response options provided depending on the nature of the question. Once satisfied with their responses, the individual will submit the form, and the completed form will be stored on ECU's EduCloud server.

Upon submission, the report is assigned a unique 16-digit identifier. This identifier is presented to the individual upon submission of the form and permits the individual to re-access the form and make modifications and/or communicate with ECU at any time. To re-access the report, the identifier must be copied and saved upon initial submission as there is no way of retrieving the identifier post-submission as it would break the anonymity of the report and the individual.

Review and follow-up of the anonymous report will be overseen by ECU's Threat Assessment Team (TAT). TAT oversees ECU's response and support services for individuals who have experienced or witnessed concerning behaviour, such as sexual or gender-based violence, harassment and bullying, discrimination and racism, and disruptive, threatening or violent behaviour. A member of TAT will intake the anonymous reports and escalate reports to administration advisors, as per Policy 3.6. The purpose of the TAT team assessment will be to determine whether the information falls within the University's scope to respond. Determinations will be made whether there is a safety concern and whether it is appropriate to take action. Representatives from the TAT team who have been provisioned accounts to access ART can also engage in messaging with the individual completing a report directly in ART and the conversation is saved to the report. Collection of data will be done to create accurate statistics on sex and gender-based violence and referral or consultation to the administrative authority if necessary. Where sufficient information exists, the ECU President may decide to take action.

When the ART is published on the ECU website in August 2024, it will be available within a series of webpages outlining how students can seek care, support and justice through ECU and other community resources.

## 2. What is the scope of this PIA?

In scope:

- Creation of ECU's ART via IT modifications to the GlobaLeaks open-source software platform.
- Hosting ART in ECU's EduCloud server and security controls for hosting and accessing ART reports stored in EduCloud.

- Information provided by unique ART reports (as disclosed by the individual reporting the sexualized violence event(s)).
- TAT's interactions with ART reports including direct access to the online tool, use of comments/interaction capabilities provided by ART, transcription and storage of notes in ECU's secure SharePoint site, use of the ART reports to further conduct health and safety assessments.
- Long term storage and retention of ART reports in accordance with ECU, FIPPA and other legislative requirements.

Out of scope:

- TAT's receipt of any identifiable reports of sexualized violence or other forms of misconduct outside of ART reports and associated policies and processes to safeguard the privacy and confidentiality of the victims and perpetrators.
- Information collected by ECU via ART that is outside of the prescribed scope of the reporting tool.
- Future uses of ART by ECU outside of the prescribed scope of the reporting tool at the time of assessment (e.g., whistleblowing).
- ART reports that are defined as out of scope of ECU's jurisdiction as per ECUAD's Policy 3.6 Sexual and Gender-Based Violence and Misconduct Policy.

### 3. What are the data or information elements involved in the initiative?

ECU students using ART will be sharing personal experiences or witnessed accounts of sex and gender-based violence and/or other forms of misconduct. Identifying information about persons affected by sex and gender-based violence and persons of interest responsible for sex and gender-based violence will be shared anonymously via the tool and stored on ECU's EduCloud server.

Review by the ECU TAT team could result in additional information being created by interacting with the information provided in the report, transcribing notes and observations and creating health and safety plans or other TAT-related assessments in response to the report. Individuals from the TAT team who have been provisioned accounts to access ART can also engage in messaging with the person completing a report directly in ART and the conversation is saved to the report.

Given the person submitting the report may include information about a perpetrator, this could involve the collection by ECU of identifying information about students, staff, or faculty at ECU or, citizens and members of Vancouver's communities.

### 4. Does the initiative include personal information?

The following information is collected via the ART and the ART questionnaire in full is provided in Appendix A:

- Time and location of incidents of sex and gender-based violence (only required field for completion in form)
- How someone was impacted by the incidents they are reporting (person harmed, witness, bystander, friend)
- Whether the person/people of concern belong to the Emily Carr University community (are they a student, employee, visitor, contractor, member of the Board of Governors, guest or a volunteer)

- If the person reporting does not know the person/people of concern, have they ever seen them before? Where and when and under what circumstances?
- A description of what happened
- Whether there is a specific reason they are filing an anonymous report at this time
- Anything else the person reporting wishes to add
- Any information that is provided via the messaging capabilities provided in ART between the person reporting and TAT

## Part 2 – Collection, Use and Disclosure

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

| **Use this column to describe the way personal information moves through the initiative step by step as if you were explaining it to someone who does not know about your initiative.** | **Collection, use, disclosure** | **FOIPPA authority** | **Personal Information** |
|---|---|---|---|
| Information about an incident of sex and gender-based violence is shared with members of the Threat Assessment Team (TAT) via the web-based ART form.<br><br>Report modifies the report (if required) post submission to include additional information or remove information via a secure 16-digit record identifier. | Collection | s. 26(c) and 26(e) | **X** |
| Information securely stored on encrypted ECU EduCloud server. | Storage/Retention | s.30 | **X** |
| Notification sent by email to select TAT team members that a new report has been submitted. | Use | s.32(a) | **X** |
| Select TAT team members log on to encrypted website to view report and make notes. | Use | s.32(a) | **X** |
| Debriefing completed between select TAT team members to determine what action, if any, can be taken based on the information reported. | Use | s.32(a) | **X** |

| | | | |
|---|---|---|---|
| Depending on the significance of the report, information may be shared by TAT members and senior policy officers (for policy 6.10 and policy 3.6) only to verify report and mitigate or intervene in risk of further sex and gender-based violence. Anonymity of reporting individual is maintained. | Use /Disclosure | s.32(a); s.32(c), s.33(2)(d); s.32(c), s.33(2)(w); s.33(2)(e) | X |
| Report is retained in ART for 7 years and then securely destroyed. | Storage/Retention | s.30 | X |

**5. Collection Notice**

If you are collecting personal information directly from the individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances). Review the sample collection notice and write your collection notice below. You can also attach the notice as an appendix.

The following collection notice will be made available before an individual completes a report:

*The personal information you record in the Anonymous Reporting Tool (ART) is collected by Emily Carr University for the purposes of responding to and preventing sexualized violence and other forms of misconduct on campus. This information is collected under the authority of s. 26(c) of the Freedom of Information and Protection of Privacy Act, R.S.BC. 1996, c. 165.*
*Should you have any questions about the collection of this personal information, please contact ECU's Privacy Officer: privacy@ecuad.ca.*

## Part 3– Storing Personal Information

**6. Is any personal information stored outside of Canada?**

No information is stored outside of Canada. All information collected by ART (reports) will be stored on ECU's EduCloud encrypted server. A PIA has been completed for EduCloud, and EduCloud is currently used by ECU to various software and service solutions in support of ECU's operations. A brief overview will be provided below[2] and more information about EduCloud is available here.

[2] https://www.bc.net/service-catalogue/shared-systems-and-technology/educloud-server

EduCloud is a virtual data centre for B.C.'s higher education institutions that is operated and supported by the University of British Columbia. This private, self-managed cloud server service offers simple and secure access to provision and manage virtual servers at a fraction of the cost of implementing physical servers. The service is available 24/7, is fully monitored, and is FIPPA compliant - securely storing all data within British Columbia (physical infrastructure located in Vancouver and Kamloops). EduCloud offers secure, multi-tenant infrastructure as a service. ECU is supplied with isolated virtual pools of compute, storage and network resources, which can be used to build and deploy robust, highly available applications and services for the institution. It is built using VMware vSphere technology, the industry-leading server virtualization platform.

Original reports will not be downloaded from ART by ECU; any notes or additional internal reports produced by TAT will be securely stored on the TAT SharePoint folder (limited access to two TAT members), which is governed under ECU's M365 PIA and stored on Canadian servers.

**7. Where and how are you storing the personal information involved in the initiative?**

See above.

**8. Does the initiative involve sensitive personal information? If yes, where and how are you storing the personal information involved in the initiative?**

Yes, sensitive personal information may be disclosed by the reporting individual. All sensitive personal information will be stored in accordance with protocols outlined in Question 6.

## Part 4 – Assessment of Disclosure Outside of Canada

*Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. Otherwise continue to Part 5.*

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

No – assessment will continue in Part 5.

| Name of service provider | Name of cloud infrastructure and/or platform provider(s) (if applicable) | Where and how is the sensitive personal information stored (including backups)? |
|---|---|---|
| | | |

**10.**

11. [illegible]

12. [illegible]

13. [illegible]

14. [illegible]

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

## Part 5 – Security of Personal Information

15. **Does the initiative involve digital tools, databases, or information systems?**
    Yes – ECU is re-designing the open-source software GlobaLeaks to create ART. Additional information is provided below.

16. **Do you or will you have a security assessment to help you ensure the initiative meets the reasonable security requirements?**

    ***Virtual Infrastructure***
    Yes – ECU IT's Security Team has configured and tested the platform to comply with ECU information security policies and standards and FIPPA requirements. Specific features offered by GlobaLeaks software, which have been configured by ECU IT are outlined in detail here, and highlighted below and in Appendix B.

    *Virtual Server*
    ECU is setting up a new virtual server in EduCloud to host the ART software. ECU is using the operating system templates pre-configured by EduCloud to meet all best practices and FIPPA requirements for security template (e.g., firewall requirements, auditing). The server will be backed up by EduCloud every 21 days and all backups are encrypted. Given previous review of EduCloud's security controls, the remaining discussion of security requirements will focus on the ART software hosting in the virtual server.

    ***ART Software – Security Controls***

*Session Management*
The session implementation follows the OWASP Session Management Cheat Sheet security guidelines. The system assigns a Session to each authenticated user. The Session ID is 256bits long secret generated randomly by the backend. Each session expires accordingly to a timeout of 60 minutes. Session IDs are exchanged by the client with the backend by means of a header (X-Session) and do expire as soon that users close their browser, or the tab running ART. Users could explicitly log out via a logout button or implicitly by closing the browser.

*Connection Anonymity*
Anonymity is offered by means of the implementation of the Tor technology. The application implements an Onion Service v3 and advises users to use the Tor Browser when accessing to it.

*Connection Encryption*
The user's connection is always encrypted, by means of the Tor Protocol while using the Tor Browser or by means of TLS when the application is accessed via a common browser. The use of the Tor Browser is recommended over HTTPS for its advanced properties of resistance to selective interception and censorship that would make it difficult for a third party to selectively capture or block access to the site.

*Network Sandboxing*
The GlobaLeaks backend integrates IP tables by default and implements strict firewall rules that restrict network incoming network connection to HTTP and HTTPS connection on Ports 80 and 443. In addition, the application makes it possible to anonymize outgoing connections that could be configured to be sent through Tor.

*Data Encryption*
All data submitted via the report including answers to questions posed by the tool, messages and metadata exchanged between individuals completing a report and ECU's TAT team is encrypted using the GlobaLeaks Encryption Protocol.

In addition to this GlobaLeaks implements many other encryption components and the following is the set of the main libraries and their main usage:

- Python-NaCL: is used for implementing data encryption
- PyOpenSSL: is used for implementing HTTPS
- Python-Cryptography: is used for implementing authentication
- Python-GnuPG: is used for encrypting email notifications and file downloads by means of PGP

*Database Security*
The GlobaLeaks backend implements a hardened local SQLite database accessed via the SQLAlchemy ORM. This design choice is selected in order to ensure that the application could fully control its configuration implementing a large set of security measures in adherence to the security recommendations by SQLite

*Secure Deletion*
The GlobaLeaks backend enables a SQLite capability for secure deletion that automatically makes the database overwrite the data upon each delete query.

*Rate Limit on User Sessions*
The system implements rate limiting on users' sessions preventing to execute more than five requests per second and applying increasing delay on requests exceeding the threshold.

*Rate Limit on Reports and Attachments*
The system implements rate limiting on reports and attachments preventing to file new submission and upload new files if the thresholds are exceeded. To note, the ability to attach any files has been disabled for ECU's implementation of the GlobaLeaks software.

Implemented thresholds are:
- Limit the number of reports that could be filed per hour: 20
- Limit the number of reports that could be filed per hour by the same IP address: 5
- Limit the number of attachments that could be loaded per hour by the same IP address: 120
- Limit the number of attachments that could be loaded per hour on a report: 30

*Browser History and Forensic Traces*
The whole application is designed keeping in mind to try to avoid or reduce the forensic traces left by individuals on their devices while filing their reports.

When the accessed via the Tor Browser, the browser guarantees that no persistent traces are left on the device of the user. In order to prevent or limit the forensic traces left in the browser history of the users accessing the platform via a common browser, the application avoids changing URI during user navigation. This has the effect to prevent the browser to log the activities performed by the user and offers high plausible deniability protection making the user appear as a simple visitor of the homepage and avoiding actual evidence of any submission.

*Secure File Delete*
Every file deleted by the application if overwritten before releasing the file space on the disk. The overwrite routine is performed by a periodic scheduler and acts as following:
- A first overwrite writes 0 on the whole file
- A second overwrite writes 1 on the whole file
- A third overwrite writes random bytes on the whole file

*Exception Logging and Redaction*
In order to quickly diagnose potential problems in the software when exceptions in clients are generated, they are automatically reported to the backend. The backend temporarily caches these exceptions and sends them to the backend administrator via email. In order to prevent inadvertent information leaks the logs are run through filters that redact email addresses and UUIDs.

*TLS for SMTP Notification*
All notifications are sent through SMTP over TLS encrypted channel by using SMTP/TLS or SMTPS, depending on the configuration.

***ART Software – User Account Controls***

*User Roles*
ART provide two separate user roles that can be configured in the system: administrator and recipient.

- Administrator
  - Holds access to the administrative panel and provides overall management of the software
  - Can adjust settings for the software (technical, administrative and security and privacy controls) and questionnaire
  - Can add, remove and modify accounts
  - Can monitor audit reports
  - Can set retention timeframes for reports
  - Cannot review reports – no viewing or editing access to submitted reports provided to administrator account
- Recipient
  - Can access and review reports
  - Can interact with individual who submitted the report via the messaging function of the tool and document feedback within the report
  - Can download the report (function will not be initiated for ECU)
  - Cannot adjust any user or software settings (only permitted for administrator accounts

Accounts will be set-up by ECU IT and ECU IT will hold the administrator accounts (two unique individuals) and two TAT members will hold recipient accounts. A back-up recipient account will also be created in case the two TAT members are both out of the office at the same time. ECU IT will set-up the accounts for TAT members and submitted temporary passwords via an encrypted message tool hosted by SFU (secret.rcg.sfu.ca). Upon initial log-in, the recipient account will be required to reset their password (see password requirements below).

To note, the ART accounts for both administrators and recipients are exclusive and not linked to ECU Active Directory accounts.

*Password Complexity*
The system enforces the usage of complex password by implementing a custom algorithm necessary for ensuring a reasonable entropy of each authentication secret. Password are scored in three levels: Strong, Acceptable, Insecure.

- Strong: A strong password should be formed by capital letters, lowercase letters, numbers and a symbol, be at least 12 characters long and include a variety of at least 10 different inputs.

- Acceptable: An acceptable password should be formed by at least 3 different inputs over capital letters, lowercase letters, numbers and a symbol, be at least 10 characters and include a variety of at least 7 different inputs.
- Insecure: A password ranked below the strong or acceptable levels is marked as insecure and not accepted by the system.

*Slowdown on Failed Login Attempts*
The system identifies multiple failed logins attempts and implement a slowdown procedure where an authenticating user should wait up to 42 seconds to complete an authentication. This feature is intended to slow down possible attacks requiring more resources to users in terms of time, computation and memory.

*Password Change on First Login*
The system enforces users to change their own password at their first login.

*Periodic Password Change*
By default, the system enforces account holders to change their own password at least every year. This period is configurable by administrators.

*Password Recovery*
In case of password loss users could request a password reset via the web login interface clicking on a "Forgot password?" button present on the login interface. ECU has enabled on the system, which means that a user clicking on the reset link would have first to insert their Account Recovery Key and only in case of correct insertion the user will be enabled to set a new password. An Account Recovery Key is only provided for the IT and TAT team accounts.

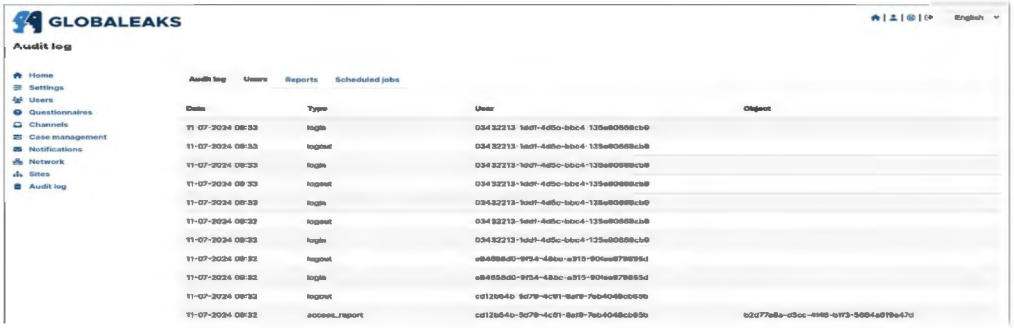
*Password Storage*
Passwords are never stored in plaintext. The platform stores user passwords hashed with a random 128- bit salt, unique for each user. Passwords are hashed using Argon2. The hash involves a per-user salt for each user and a per-system salt for report.

***ART Software – Auditing***

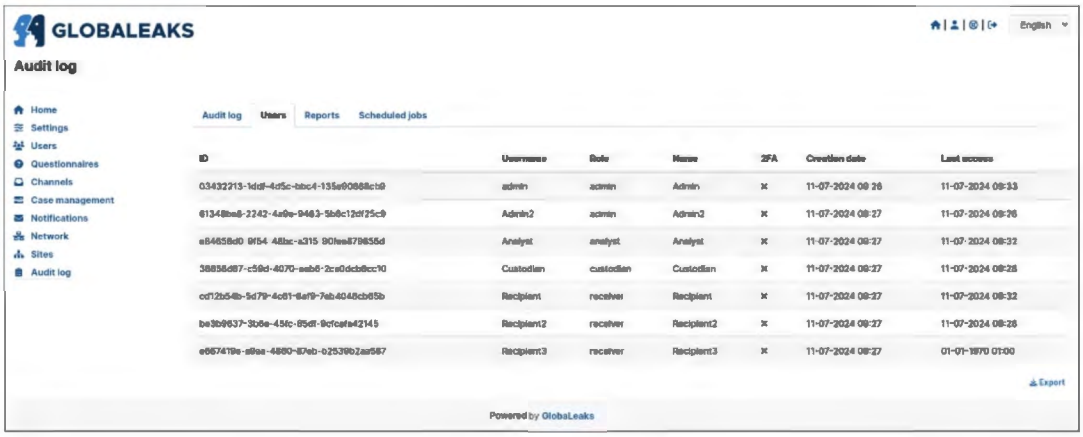
The software features a privacy preserving audit log enabling administrators of the system to supervise user and reporting activities. Only administrators can access the audit logs via the administrator dashboard. Logs will be reviewed in ART and no files will be exported outside of ART. ECU IT will engage in retrospective audits should there be any concerns flagged by the TAT team or as reported otherwise from other members of the ECU community.

The following screenshots outlined the elements captured by each of the available audit logs.

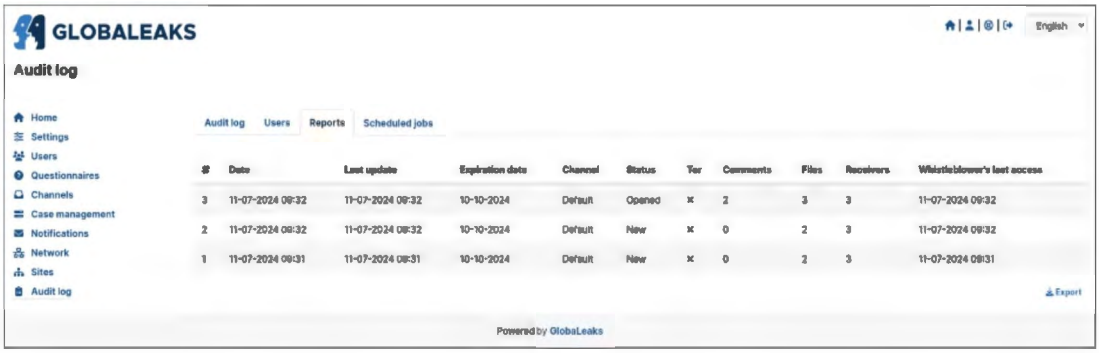
Audit Log:




User Activities:




Report Activities:



17. **Controlling and tracking access - Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.**

| Strategy | Yes / No and please describe |
|---|---|
| **We allow employees only in certain roles access to information** | Yes, only select members of the Threat Assessment Team will be provisioned a "recipient" account to review and intake reports.<br><br>At most two ECU IT representatives will hold "administrator" accounts.<br><br>Both teams will engage in regular review of the accounts / roles and the TAT team will notify ECU IT where accounts need to be de-commissioned should team members change. |
| **Employees that need standing or recurring access to personal information must be approved by the appropriate authority** | Yes, only individuals with a need to know for the purposes of their job description will be provisioned an account. Oversight of TAT accounts will be provided by the Program Manager, Violence Reduction + Incident Response. Oversight of ECU IT accounts will be provided by the Manager, Institutional Research + Applications. |
| **We use audit logs to see who accesses a file and when** | Yes. User access will be logged according to date/time of access (see User Activities audit log above). |
| **Additional strategies:** | See sections above regarding technical and administrative controls. |

## Part 6 – Accuracy, Correction + Retention

*In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.*

18. **Do you have a process in place to correct personal information?**

    The personal information submitted is submitted completely anonymously. ECU will not be able to correct information after it is submitted by the individual who reported it; however, the individual can access their report and update information submitted in the report using the unique 16-digit reference number.

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

The information submitted by an anonymous reporter can be used to identify and prevent risk to individual and collective well-being and safety. This, however, is determined on a case-by-case basis. Some anonymously reported information may be enough to enable the TAT team to take action that can affect an individual, however, in some cases, there will not be enough information to take action that can prevent risk.

The TAT team may also use the information to make a decision about the perpetrator and whether additional action will be taken in accordance with TAT review, assessment and subsequent policies and procedures for escalating review including ECU Policy 6.10 *Dealing with Threatening Behaviour*; 6.10.1 *Threat Assessment Team Procedures* and 3.6.*1* *Sexual And Gender-Based Violence And Misconduct Procedures for Students*.

**20. Do you have a retention schedule in place related to personal information used to make decisions? Retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

Information shared through the ART will be treated as TAT files and kept for a maximum of seven years, then destroyed. TAT team members will work with ECU on establishing this process in accordance with ECU's Records Retention Schedule.

## Part 7 – Additional Risks

*In the table below describe any additional risks that arise from collecting, using, disclosing, or storing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.*

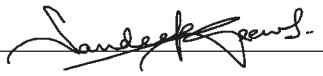
| Possible Risk | Response |
|---|---|
| Risk 1: Reporter could be identified either via the information provided in the report and/or if action is taken by TAT on reported information. | Before completing the report, a standard collection notice is provided along with an explicit description of the types of information the reporter should / should not provide in the report. ECU has also limited the number of free text boxes to minimize the ability for reporters to disclose ancillary information to ECU when completing the report.<br><br>Nevertheless, ECU cannot completely prevent the disclosure of personal information by reporters. Should the reporter submit information that could lead to their identification, the reporter is actively providing their consent for the collection of this information. All information provided by the reporter will be treated as personal information and protected in accordance with ECU's policies and procedures.<br><br>TAT members have no way of knowing or verifying who reported, as the form doesn't ask for the person to identify themselves. TAT will treat the information in accordance with ECU's Policy 3.6 and other institutional policies and procedures. |
| Risk 2: Notes on ART reports are reviewed by an individual without | Only two TAT team members will have direct access to ART via separate account logins. |

| Possible Risk | Response |
|---|---|
| authorization to access and view ART reports. | All access and interaction with ART reports will be via ART; no local downloads are permitted. All activities on ART are logged and available for auditing purposes by the administrator accounts.<br><br>The TAT team members will keep notes taken on ART reports secure in their offices and via the team's secure SharePoint folder and will shred/delete them once they are no longer needed (in accordance with ECU Records Retention Schedule). |
| Risk 3: Students or other ECU community members may use ART to report activities outside of the prescribed scope of ART leading to unauthorized collection of personal information by ECU. | A standard collection notice is provided along with an explicit description of the types of information the reporter should / should not provide in the report. ECU has also limited the number of free text boxes to minimize the ability for reporters to disclose ancillary information to ECU when completing the report.<br><br>Nevertheless, ECU cannot completely prevent the use of ART to report other activities outside its intended scope. Should the reporter submit a report that is outside of ART's intended purpose / scope, the TAT team will determine how to handle the report in accordance with ECU's institutional policies and procedures and will escalate or destroy the report accordingly. |
| Risk 4: No standard ECU Privacy Notice on website to link to via the ART tool | As ART may collect personal information, the tool provides the option of linking to the institution's external facing privacy notice. ECU does not have a standalone privacy notice on its website and currently provides a PDF of an internal Information Protection policy (hidden within other governance documents). ECU to update the general ECU website with an appropriate privacy notice that covers collection, use and disclosure of personal information via electronic websites overseen by ECU. |

Please ensure Parts 7 and 8 are attached to your submitted PIA.

## Part 8 – Program Area Signatures

*This PIA is based on a review of the material provided to the Privacy Office as of the date below. If, in future any substantive changes are made to the scope of this PIA, a PIA Update must be completed and submit it to Privacy Office.*

| | | |
|---|---|---|
| *Department Manager* | Signature | Date |
| Sandeep Sidhu |  | 15 Aug 2024 |
| **Sandeep Sidhu**<br>*Chief Information Officer* | Signature | Date |
| **Adrian Tees**<br>*Privacy Officer* | Signature | Date |

A final copy of this PIA (with all signatures) must be delivered to privacy@ecuad.ca for record keeping.

# Policy 3.6 SGBV Anonymous Report Form

## *Privacy Overview*

The personal information you disclose in the Anonymous Reporting Tool (ART) is collected by Emily Carr University (ECU) for the purposes of responding to and preventing sexualized violence and other forms of misconduct on campus. This information is collected under the authority of s. 26(c) of the Freedom of Information and Protection of Privacy Act, R.S.BC. 1996, c. 165.

As this form is intended to keep the individual reporting anonymous, please do not include any personal information that could identify you in your responses. The privacy and confidentiality of the information you disclose in the reporting form will be governed in accordance with ECU's Privacy Policy, Information Security Policy and supporting standards and guidelines.

Should you have any questions about the collection of this personal information, please contact: privacy@ecuad.ca

## *Form Overview*

Thank you for reaching out to share this important information.

The purpose of this is for ECUAD to assess health and safety concerns, determine if we can mitigate risk and plan health and safety responses.

Any information provided can help the university intervene early, provide support and plan prevention.

Please provide as much information as possible about the incidents you wish to report.
You can submit information about a single incident, or multiple incidents.

You are free to skip any questions you do not wish to answer, except date/time/location.

This information is helpful in responding and safety planning.

At the end of this section there will be space for you to add anything you feel is important that was not conveyed in answering the questions.

**Definition:**
Person/People of concern means the people responsible for causing harm you are making this report about.

**INCIDENT INFORMATION**

Date, Time and Location for all incidents you wish to report
(E.G. DD/MM/YYYY; 12:00 pm; Vancouver, B.C.) (*Required)
How are you impacted by the incidents reported here?

- ☐ Person Harmed

- ☐ Witness
- ☐ Bystander
- ☐ Friend

Is the person/people of concern a current member of the Emily Car University community?

- ☐ Student (s)
- ☐ Employee (faculty, staff, administration)
- ☐ Visitor to Campus
- ☐ Contractor
- ☐ Member of the Board of Governors
- ☐ Guest
- ☐ Volunteer

If you do not know the person/people of concern, have you ever seen them before? If so, where, when and under what circumstances?

Please describe what happened.

Is there a specific reason you are filing an anonymous report at this time?

Is there anything else about what happened that you would like to add?

***POP UP MESSAGE UPON COMPLETION***

Thank you for sharing this information with us about your experience.

This response confirms that your incident was sent anonymously to the Threat Assessment Team.

**DOWNLOAD A COPY OF YOUR RESPONSES BELOW**

A member of the Threat Assessment Team will review your information in the next three business days to determine what action, if any, can be taken.

**If you need immediate support, please consider accessing the following resources:**

**Emily Carr University of Art and Design Counselling Team**

Counsellors in Student Wellness can provide confidential, safe counselling free of charge.

To book an appointment email counselling@ecuad.ca

**Support for Reporting Sex and Gender-Based Violence in the in the Community**
**Salal Sexual Violence Support Centre**

Local: 604-255-6344
Toll-free: 1-877-392-7583
Website: https://www.salalsvsc.ca/

**Support for Care in the Community**

- Vancouver General Hospital – Sexual Assault Service
  899 West 12th Avenue, Vancouver, B.C., V5Z 1M9
  T: 604-875-2881
- Urgent Care Center UBC Hospital - Sexual Assault Service
  2211 Wesbrook Mall, Vancouver, B.C., V6T 2B5
  T: 604-822-7121
- Surrey Memorial Hospital: Embrace Clinic (at the Shirley Dean Pavilion)
  9634 King George Blvd, Surrey, B.C., V3T 0G7
  T: 604-807-5406
- Abbotsford Regional Hospital, Forensic Nursing Service
  32900 Marshall Road, Abbotsford B.C., V2S 0C2
  604-851-4700 x 646147

**Making a Police Report**
**VPD Sex Crimes Unit Contact Information**
If you need to make a police report, please call the VPD non-emergency line at 604-717-3321 or 911 for an in-progress or recent crime. (604) 717-2634 scu@vpd.ca

## Appendix B – GlobaLeaks Configurable Features

### User Features

- ☐ Multi-user system with customizable user roles (whistleblower, recipient, administrator)
- ☐ Entirely manageable from a web administration interface
- ☐ Support for **more than 90 languages** with support for Right-to-Left (RTL)
- ☐ Let whistleblowers decide if and when to confidentially declare their identity
- ☐ Exchange multimedia files with whistleblower
- ☐ Secure management of files' access and visualization
- ☐ Chat with Whistleblower to discuss the report
- ☐ Unique 16-digit receipt for the whistleblower to log back in anonymously
- ☐ Simple recipient interface for receiving and analyzing reports
- ☐ Support for the categorization of the reports with labels
- ☐ Support for the user search of reports
- ☐ Support for assigning and creating case management statuses
- ☐ Customizable look and feel (logo, colour, styles, font, text)
- ☐ Define multiple reporting channels (e.g. per-topic, per-department)
- ☐ Create and manage multiple whistleblowing site (e.g for subsidiaries or third party clients)
- ☐ Advanced questionnaire builder
- ☐ Whistleblowing system statistics

### Legal Features

- ☐ Designed in adherence with **ISO 37002:2021** and **EU Directive 2019/1937**
- ☐ Bidirectional anonymous communication (comments/messages)
- ☐ Customizable case management workflow (statuses/sub-statuses)
- ☐ Whistleblower identity conditional reporting workflow
- ☐ Manage conflict of interest in the reporting workflow
- ☐ Custodian functionality to authorize access to whistleblower identity
- ☐ GDPR privacy by design and by default
- ☐ GDPR configurable data retention policies
- ☐ GDPR compliant subscriber module for new users of SaaS services
- ☐ No logs of IP addresses
- ☐ Audit log
- ☐ Integratable with existing enterprise case management platform
- ☐ Free Software OSI Approved **AGPL 3.0 License**

### Security Features

- ☐ Designed in adherence with **ISO 27001:2022**
- ☐ Full data encryption of whistleblower reports and recipient communication
- ☐ Digital anonymity support with **Tor** integration
- ☐ Built-in HTTPS support with **TLS 1.3** standard (**SSLabs A+** rating)
- ☐ Automatic free digital certificate enrollment (**Let's Encrypt**)
- ☐ Multiple penetration tests with full public reports
- ☐ Conform to industry standards and best practices for application security (**OWASP**)
- ☐ Two-Factor authentication (2FA) support compliant with standard **TOTP RFC 6238**
- ☐ Integrated network sandboxing with iptables
- ☐ Integrated application sandboxing with **AppArmor**
- ☐ Complete protection against automated submissions (spam prevention)
- ☐ Subject to continuous peer-review and periodic security audits

- PGP support for encrypted email notifications and encrypted file downloads
- Does not leave traces in browser cache

**Technical Features**

- Multi-site support enabling to run multiple virtual site on the same setup
- Responsive user interfaces made with **Boostrap** CSS Framework
- Built-in Accessibility Support with **WAI-ARIA** compliance
- Automated Software Quality Measurement and Continuous Integration Testing
- Long-Term Support plan (LTS)
- Built with lightweight framework technologies (**AngularJS** and **Python Twisted**)
- Integrated **SQLite** database
- Automatic setup of **Tor Onion Services Version 3**
- Support for self-service signup for whistleblowing SaaS service setup
- Support for Linux operating system (**Debian**/**Ubuntu**)
- Debian packaging with repository for update/upgrades
- Fully self-contained application
- Easy integration of the platform with existing websites
- Rest API