COMMUNITY SERVICES

2.10.0 Privacy Program Overview

Scope:

PLEA is responsible for managing personal information from multiple stakeholders, including employees, clients, family caregivers, students, volunteers, donors and the Board of Directors. PLEA is committed to protecting personal information, and to continually improving its privacy management practices. As part of this commitment, PLEA has a privacy program which is reviewed on an annual basis.

All 2.10 Privacy-related policies are available on PLEA's website as well as on the agency's internal Shared drive.

PLEA's privacy program is overseen by the Privacy Officer, who is responsible for:

- Developing, providing guidance on and maintaining privacy policies/initiatives
- Ensuring privacy training is included in the onboarding procedures
- Providing guidance to managers and employees on privacy-related issues
- Responding to requests for access to and correction of personal information
- Supporting managers in handling privacy complaints, information incidents and privacy breaches
- Working with the Information and Privacy Commissioner when necessary

Contact Information for PLEA's Privacy Officer:

Michelle Hawco, Privacy Officer
604-708-2626
privacy@plea.bc.ca

Statements:

1. PLEA values the trust of those it works with and recognizes that maintaining that trust requires that all information in its control or custody be protected.

2. PLEA is committed to taking measures to protect all confidential records, whether in electronic or paper copy.

3. The purpose of this policy is to provide employees with guidance in using electronic and physical safeguards to protect the confidential information that the agency collects and uses from unauthorized access.

4. PLEA expects all employees to make reasonable efforts to ensure that personal information in their care and custody is managed with care.

5. PLEA's privacy practices are consistent with the requirements of legislation, funders, accreditation standards and the Canada Revenue Agency.

Components of PLEA's Privacy Management Program:

Training Initiatives and Performance Management

- **Privacy training.** Occurs during the onboarding process, as well as annually as part of the Annual Learning Plan, and when determined as necessary by the manager.
    - *Privacy training at onboarding* is facilitated by the manager. This training includes both the completion of the MCFD or CLBC Privacy Training and a review of all 2.10 privacy-related policies.
    - *Annual privacy training* is coordinated by the Manager of Impact Evaluation and Quality Assurance, as part of the Annual Learning Plan. This training consists of a review of all 2.10 privacy-related policies.

- **Cyber security training.** Occurs during the onboarding process and ongoing thereafter. Completion of this training is coordinated by the Manager of Impact Evaluation and Quality Assurance, as part of the Annual Learning Plan.

- **Participant privacy training.** The rights of persons served, including the right to privacy, are reviewed with participants during the intake process.
    - During the intake process, privacy-related brochures are provided to participants to ensure the relevant content within privacy policies is presented in a format that is easy to read and access.

- **Performance evaluations.** Evaluations assess employees' ongoing efforts to maintain privacy and confidentiality.

Privacy-related policies

- *Schedule F, Information Management (Records Privacy and Security)*
- *1.5.2 Responding to Legal Action*
- *1.5.3 Confidentiality of Records*
- *2.2.7 Donor Information & Records*
    - *Appendix 2.2.7A Our Guiding Principles for Safeguarding Donor Information*
- 2.10 Privacy-related policies
    - *2.10.1 Personal Information Management* policy
        - *Appendix 2.10.1A Confidentiality Agreement* (this is completed prior to the employee's first day, as well as each time they start a new position)
    - *2.10.2 Information Incident Management* policy
    - *2.10.3 Requesting Correction of Personal Information Policy*
        - *Appendix 2.10.3A Request to Correct Personal Information Form*
    - *2.10.4 Privacy Audits Policy*
        - *Appendix 2.10.4A Privacy Audit Form*
- 2.4 Technology-related policies
    - *2.4.0 Technology*
    - *2.4.1 Acceptable Use*
    - *2.4.2 Hardware and Software Acquisition and Disposal*
    - *2.4.3 Backup and Disaster Recovery*
    - *2.4.4 Security and Confidentiality – Servers*
    - *2.4.5 Security and Confidentiality – Access*
    - *2.4.6 Security and Confidentiality – Internet*
    - *2.4.7 Security and Confidentiality – Passwords*
    - *2.4.8 Security and Confidentiality – Third Party Service Delivery*
    - *2.4.9 Assistive Technology*
    - *2.4.10 Protection Against Cyber Security Threats*
- *3.1.21 Personnel File Policy* & *Appendix 3.1.21 Personnel File Copy/Review Request Form*
- *3.4.1 Practicum Student Program Policy*

2.10.1 Personal Information Management

Scope:

This policy applies to all PLEA employees or candidates for employment, independent contractors, participants, students and volunteers. It applies to the management of personal information in any form, whether oral, electronic or written.

This policy is based on the British Columbia's *Personal Information Protection Act* (PIPA), which is intended to balance an individual's right to protect their personal information with an organizations' need to collect, use or disclose personal information for reasonable purposes. The Freedom of Information and Protection of Privacy Act (FOIPPA) covers all personal information in the custody or control of a ministry, as defined in the individual program's funding contracts/privacy schedules.

This policy is intended to be a guide for individuals and is not inclusive of all privacy obligations detailed in individual programs' funding contracts/privacy schedules, including *Schedule F, Information Management (Records Privacy and Security)*. Individuals should refer to their program's policy and procedures manual, and consult with their supervisor, for the specific privacy requirements of their program.

Donors should refer to *2.2.7 Donor Information & Records* for information related to managing the personal information of donors.

This policy should be read in conjunction with all policies listed in the *2.10.0 Privacy Program Overview* policy.

Statements:

1. PLEA is committed to protecting the personal information within its custody, including the personnel files for employees, volunteers, and independent contractors.

2. In accordance with current privacy legislation, PLEA collects only personal information that is necessary to operate its programs, services and activities. Records are held and disposed of securely, and access is limited on a need-to-know basis.

3. The agency makes every reasonable effort to protect personal information, regardless of its format, including paper, electronic, audio and video data.

4. Employees in programs providing direct services to participants should contact their manager prior to collecting, securing, using, retaining or disclosing personal information to ensure that the specific privacy obligations within their program's funding contracts are met.

5. PLEA is unable to disclose personal information to parties outside of Canada.

6. This policy is built on the ten principles of privacy protection (i.e., "Fair Information Practices"), set of guidelines, recommended by the Office of the Information and Privacy Commissioner, regarding the

Charitable Registration
10781 0467 RR0001
bcgeu

collection, security, use and disclosure of personal information. The ten principles of privacy protection are:

(1) Principle 1 – Be Accountable
(2) Principle 2 – Identify the Purpose for the Collection of Personal Information
(3) Principle 3 – Obtain Consent for Collection, Use or Disclosure of Personal Information
(4) Principle 4 – Limit the Collection of Personal Information
(5) Principle 5 – Limit the Use, Disclosure, and Retention of Personal Information
(6) Principle 6 – Ensure the Accuracy of Personal Information
(7) Principle 7 – Reasonable Security
(8) Principle 8 – Be Open and Transparent
(9) Principle 9 – Right of Access and Correction
(10) Principle 10 – Provide Recourse

Definitions:

Collection: the act of gathering, acquiring, recording, or obtaining personal information from any source, including third parties, by any means.

Consent: a voluntary agreement to have an individual's personal information collected, used and disclosed for a defined purpose. Consent can be either express or implied and can be provided directly by the individual or by an authorized representative.

- *Express consent* can be given orally, electronically or in writing, but it is always unequivocal and does not require any inference on the part of the agency.
- *Implied consent* is consent that can reasonably be inferred from an individual's actions or inaction.

Disclosure: making personal information available to a third party.

Employee Personal Information: personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment.

Individuals: for the purposes of this policy, *individuals* include persons associated with PLEA who control personal information related to the operations of the agency, or whose personal information is controlled by PLEA. *Individuals* may include:

- Employees or candidates for employment;
- Independent contractors;
- Participants;
- Students; and
- Volunteers.

Personal Information: information about an identifiable individual, other than business contact information, that is recorded in any form.

Reasonable purposes: under PIPA, reasonable means what a reasonable person would think is appropriate in the situation. What is reasonable will depend on factors such as the kind or amount of personal information collected, the plan to use that information, and where or to whom the information is disclosed.

Supervisor: the person overseeing the individual's involvement with PLEA. Examples include managers, Volunteer Coordinators (for volunteers) and Services Coordinators (for Family Caregivers).

Third Party: a person or organization outside of PLEA.

Use: the treatment, handling and management of personal information by and within the organization.

Responsibilities:

Individuals are responsible for:

a. Using the procedures within this policy to guide their personal information management practices.
b. Consulting with program policies for specific procedures required under the relevant funding contract before taking action.
c. Understanding their rights and responsibilities under this policy.
d. Understanding the limitations to the ten principles of privacy protection (e.g., the duty to report), where applicable.
e. Relaying information to participants on the rights of persons served, informed consent and complaint procedures, where applicable.
f. Asking their supervisor questions when they are uncertain about their role in protecting personal information.

The supervisor is responsible for:

a. Contributing to a privacy-centered culture (e.g., modeling the ten privacy principles in their daily practice and taking action when the principles are not embodied by those they oversee)
b. Ensuring individuals are aware of how the ten privacy principles apply to their work:
    i. At the commencement of their involvement with PLEA.
    ii. When a new or updated version of this policy is issued.
c. Annually reviewing the ten privacy principles with their individuals or teams.
d. Investigating complaints, in consultation with the Privacy Officer, where appropriate.

The Privacy Officer is responsible for:

a. Providing guidance on privacy-related matter to individuals.
b. Receiving complaints and referring them to the supervisor to investigate, where appropriate.
c. Recording all privacy complaints and corrective measures taken and reporting that information at least annually to the Executive Director.

The Executive Director, or their designate, is responsible for:

a. Informing the Board of Directors at least annually of the number and type of privacy complaints reported, and corrective measures taken.

Procedures:

Being Accountable

1. The agency is responsible for protecting all personal information within its control (e.g., participant files or personnel file records). This includes personal information shared with or transferred to another organization.

Identifying the Purpose for Collection of Personal Information

2. The reasons why the agency is collecting personal information must be identified and disclosed in writing to those providing personal information. This includes the agency's legal authority for collecting the information as well as the contact information of a person who can answer questions about the collection of information. This information should be clearly communicated on forms requesting information.

3. Personal information will only be collected for the purposes of:
    a. Establishing, managing or terminating a relationship with employees, independent contractors (e.g., Family Caregivers), participants, students and volunteers; or

b. Meeting legal, regulatory or contractual requirements.

Limiting Collection of Personal Information

4. Personal information shall only be collected when the agency has a reasonable purpose and legal authority for doing so.

5. The collection of an individual's personal information is limited to that which is necessary for the purposes identified.

Obtaining Consent for Collection, Use or Disclosure of Personal Information

6. Consent from the individual whose personal information is being collected, used, or disclosed is obtained before the agency can collect, use or disclose such information, except in the following circumstances:
    a. Where the purpose for collecting using or disclosing the personal information would be considered obvious and the individual voluntarily provides personal information for that purpose.
    b. When the collection, use or disclosure of personal information is permitted or required by law;
    c. In an emergency that threatens an individual's life, health, or personal security;
    d. When the personal information is available from a public source (e.g., a telephone directory);
    e. When PLEA requires legal advice from a lawyer;
    f. For the purposes of collecting a debt;
    g. To protect the agency from fraud; or
    h. To investigate an anticipated breach of an agreement or a contravention of law.

7. Subject to certain exceptions (e.g., the personal information is necessary to provide services or the withdrawal of consent would frustrate the performance of a legal obligation), individuals can withhold or withdraw their consent for the agency to use their personal information.

8. Individuals must provide written and explicit consent for the agency to use or disclose their personal information for secondary purposes.

Limiting Use, Disclosure and Retention

9. Personal information may only be used or disclosed for the reasons identified when it was collected or under another legal authority (e.g. *the Freedom of Information and Protection of Privacy Act, or FOIPPA).* Individuals must provide new consent to use or disclose information when information is needed for a second purpose.

10. Access to personal information is limited to individuals with a need-to-know basis (e.g. employees whose duties reasonably require the information). This includes managers who require the information for the purposes of establishing, managing or terminating an employment relationship.

11. Personal information that was used to make a decision about an employee is retained for at least two years following the decision, with the exception of the successful candidate's interview notes which are saved to their personnel file.

12. Personal information is destroyed, erased or made anonymous as soon as it is no longer required for a legal or business purpose. Destruction methods include cross-shredding information (using a confidential shredding service) or removing electronically stored information.

Reasonable Security

13. The agency makes reasonable security arrangements (physical, technical and procedural) to protect personal information that are proportional to the sensitivity of the information. Please see the 2.*4 Technology* policies for more information.

14. The agency protects the personal information it discloses to third parties under contractual agreements by stipulating the confidentiality requirements of the information and the purposes for which it can be used.

15. All PLEA employees with access to personal information are required, as a condition of employment, to respect the confidentiality of personal information. Employees review and sign Appendix 2.10.1A *Confidentiality Agreement* prior to commencing their involvement with PLEA (i.e., prior to their first day).

Transparency

16. The following will be made available to an individual upon request:
    a. The title and contact information of PLEA's Privacy Officer;
    b. The process to follow to gain access to their personal information; and
    c. Information that explains PLEA's personal information practices, such as this policy.

Ensuring Accuracy

17. When personal information is being used to make a decision about an individual, the agency takes reasonable steps to ensure it is accurate and complete.

18. The agency updates the personal information within its control when necessary to fulfil the information's purpose or upon notification by the individual.

Right of Access and Correction

19. Individuals have a right to access and correct their personal information, subject to limited exceptions. Please see the *2.10.4 Requesting Correction of Personal Information* policy for additional information on requesting corrections to personal information.

Recourse for Privacy Complaints

20. Individuals making a complaint related to the use of their personal information must do so in writing, by emailing the Privacy Officer, Michelle Hawco (privacy@plea.bc.ca) directly. Complaints should include at least the following:
    a. Their contact information (i.e., name, phone number and email address).
    b. A description of the personal information inappropriately accessed, collected, used or disclosed.
    c. The consequences of the breach (e.g., identity threat)
    d. The remedy sought.
    e. Any supporting documentation.

21. The Privacy Officer will acknowledge receipt of the complaint and may refer the complaint to the supervisor to investigate, where appropriate. Supervisors who receive complaints must inform the Privacy Officer.

22. The designated investigator will investigate all complaints received, in consultation with the Privacy Officer. If necessary, the investigator will contact the individual to clarify the complaint during the investigative process.

23. If substantiated, the supervisor shall take appropriate action to resolve the complaint.

24. The investigator or Privacy Officer will notify the complainant of the outcome of the investigation and explain the corrective measures taken, where applicable.

25. The investigator or Privacy Officer will inform individuals of their right to contact the Information and Privacy Commissioner if they are not satisfied with the agency's response to the complaint.

Confidentiality

26. All reasonable efforts are made to keep complaints and investigations under this policy confidential. Individuals who are interviewed in relation to a complaint or investigation must not disclose the allegations, evidence or other information they learn during the investigation or complaint process with anyone, including other parties or witnesses involved.

Duty to Report

27. The duty to report is an exception to the privacy principles related to the use and disclosure of personal information. PLEA's obligation to protect confidentiality of personal information does not apply when disclosure is necessary to prevent serious, foreseeable, and imminent harm to another individual.

28. Individuals are expected to disclose to their supervisor immediately, and follow their instructions, if:
    a. They suspect another individual is being harmed, may harm themselves or may harm others.
    b. They have reason to believe a child has been, or is at risk for, abuse or neglect.
    c. An individual's actions or intentions pose a risk to the life, health or security of themselves or others.

Responding to Legal Action (i.e., police investigations)

29. Please refer to the *1.5.2 Responding to Legal Action* policy for additional information on the steps employees take in the event of a subpoena, search warrant or investigation.

Documenting and Reporting Privacy Complaints

30. A secure filing system is maintained by the Privacy Officer for complaints made pursuant to this policy and the investigation process.

31. The Executive Director informs the Board of Directors at least annually of the number and type of privacy complaints received and corrective measures taken.

2.10.2 Information Incident Management

Scope:

This policy applies to all PLEA employees or candidates for employment, independent contractors (e.g., Family Caregivers and Respite Family Caregivers), and volunteers. It applies to the management of personal information in any form, whether oral, electronic or written.

Individuals should refer to their program's/department's policy and procedures manual for the specific privacy requirements of their program/department. Donors should refer to *2.2.7 Donor Information & Records* for information related to managing the personal information of donors.

This policy should be read in conjunction with *2.10.1 Personal Information Management* policy, which details the procedures for the collection, use, disclosure and destruction of personal information, and all other policies listed in the *2.10.0 Privacy Program Overview* policy.

Statements:

1. PLEA is the steward of confidential information, including the personal information of employees or candidates for employment, independent contractors, participants, and volunteers. PLEA employees, volunteers, and independent contractors must protect personal information in accordance with the requirements set out in the *Personal Information and Protection Act – Province of British Columbia* (PIPA) and ensure that if an information incident occurs, it is managed in an appropriate manner.

2. This policy is intended to guide the response to and mitigation of risks arising from actual or suspected information incidents, including privacy breaches.

3. PLEA's Privacy Officer is available to provide management and employees with advice, support and investigation services to assist them in navigating the information incident process.

Definitions:

Affected Individuals: for the purposes of this policy, *affected individuals* may include persons associated with PLEA whose personal information is controlled by PLEA. They may include:

- Employees or candidates for employment;
- Participants;
- Independent contractors (e.g., Family Caregivers and Respite Family Caregivers);
- Students;
- Volunteers; and
- Donors.

Supervisor: the person overseeing the individual's involvement with PLEA. Examples include managers, Volunteer Coordinators (for volunteers) and Services Coordinators (for Family Caregivers and Respite Family Caregivers).

Individuals: for the purposes of this policy, *individuals* include persons associated with PLEA who control personal information related to the operations of the agency. *Individuals* may include:

- Employees or candidates for employment;
- Independent contractors (e.g., Family Caregivers and Respite Family Caregivers);
- Students; and
- Volunteers.

Information Incident: is a single or a series of events involving the collection, storage, access, use, disclosure, or disposal of information that threaten privacy or information security and/or contravene law or policy.

Personal Information: recorded information about an identifiable person other than business contact information.

Privacy Breach: the theft or loss, or the access, collection, use or disclosure of personal information that is not authorized. A privacy breach is a type of information incident.

Roles and Responsibilities:

Individuals are responsible for:

a. Being aware of their responsibilities under this policy.
b. Reporting to their supervisor or the Privacy Officer as soon as they become aware of, or suspect, a potential information incident or privacy breach.
c. Taking appropriate steps to contain an incident and recover any information as directed by the supervisor or Privacy Officer as appropriate.

The supervisor is responsible for:

a. Ensuring individuals are aware of their responsibilities under this policy:
    i. At the commencement of their involvement with PLEA.
    ii. When a new or updated version of this policy is issued.
b. Annually reviewing the ten privacy principles with their individuals or teams.
c. Notifying the Privacy Officer of any privacy breaches or information incidents that are reported to them.
d. Investigating all reports of privacy breaches, in consultation with the Privacy Officer.
e. Taking immediate action to resolve the issue, mitigate risks and/or prevent reoccurrence.
f. Notifying the person(s) affected by the information incident or privacy breach, where appropriate.

The Human Resources department is responsible for:

a. Storing information related to a privacy breach/information incident securely.
b. Tracking and retaining information about the agency's response to an information incident.
c. Reporting on information incidents on behalf of the agency.

The Privacy Officer is responsible for:

a. Providing guidance on privacy-related matter to individuals.
b. Recording all information incidents and privacy breaches, and reporting that information at least annually to the Executive Director.

The Executive Director is responsible for:

a. Informing the Board of Directors at least annually of the number and type of privacy breaches and information incidents reported, and corrective measures taken.

Procedures:

Reporting Privacy Incidents

1. Individuals must *immediately* report any actual or suspected information incidents to:
    a. their supervisor; and/or
    b. PLEA's Privacy Officer (Michelle Hawco) by calling 604-708-2626 or by emailing privacy@plea.bc.ca.

2. The requirement to report immediately includes actual or suspected information incidents discovered outside of normal working hours.

3. Where PLEA's Privacy Officer determines the incident is outside of their mandate, the Privacy Officer must provide notice of the incident to the Executive Director.

Preliminary Assessment

4. The Privacy Officer must conduct a preliminary assessment of reported information incidents that includes but is not limited to, the following:
    a. Whether the incident falls within the Privacy Officer's mandate.
    b. The type of information involved, including whether personal information is involved.
    c. The potential severity of the incident.
    d. The likelihood that an actual information incident has occurred.

Containment and Recovery

5. In the event of an information incident, PLEA must take appropriate steps to contain the incident and, wherever possible, recover any information that has been lost of otherwise exposed.

6. These steps will vary depending on the nature of the incident, but could include:

    a. Isolating or suspending the activity that led to the incident.
    b. Correcting weaknesses in physical or technical security.
    c. Recovering or seeking the disposal of any information or IT equipment that was lost, stolen, or otherwise exposed.
    d. Determining if any copies of confidential information where made or shared with third parties and attempting to recover them where possible.
    e. Requesting that individuals involved provide written attestations confirming that they have returned and or destroyed any records they received without authorization, and whether they sent them to others and, if so, to whom.

Privacy Breach Harm Assessment and Notification

7. In consultation with the Privacy Officer, the supervisor must ensure that a harm assessment is completed for all privacy breaches in order to determine the risk of harm to affected individuals as a result of the incident.

8. Harm assessments must consider informational and situational factors, in addition to the circumstances of the incident. This includes, but is not limited to:

    a. Which and how many individuals are affected.
    b. The sensitivity, context, and volume of the personal information involved.
    c. The ability to quickly contain the incident and the potential likelihood of further dissemination of the information involved.
    d. The relationship between the party in receipt of personal information and the person the information is about (i.e., affected individual).

e. Whether any affected individuals could face a risk of:
    i. identity theft or identity fraud;
    ii. physical harm;
    iii. financial, business, or employment loss;
    iv. hurt, humiliation or damage to reputation; and/or
    v. loss of trust
    vi. whether legal or contractual obligations require notification.

9. In determining the risk of harm to an affected individual, the weight applied to each factor above should be determined according to the circumstances of the incident.

10. The supervisor notifies the individual(s) affected by the information incident if the risk of harm, as a result of the breach, outweighs the risk of further harm to an individual, if notification occurs. Such notifications should occur without unreasonable delay, be direct wherever possible, and should include the following information:

    a. The date of the privacy breach.
    b. A description of the privacy breach.
    c. The personal information involved.
    d. The risk to the affected individual and the steps taken to mitigate the potential for harm.
    e. Steps the affected individual can take to further mitigate any potential harm they face.
    f. Measures that have been, or will be, taken to prevent similar incidents from occurring in the future.
    g. The contact information of the Privacy Officer who can answer questions or provide further information.
    h. Their right to complain to the Office of the Information and Privacy Commissioner (OIPC) or notice that the OIPC is aware of the breach and contact information for the OIPC.

Investigations

11. The supervisor investigates all reports of privacy breaches, in consultation with the Privacy Officer, to determine the nature, extent, and/or cause of an information incident.

12. The Human Resources department may be consulted for their subject matter expertise (e.g., administrative fairness) in the investigative process.

13. The Executive Director, and relevant stakeholders, are notified as applicable.

Documenting the Information Incident/Privacy Breach

14. A secure filing system will be maintained by the Human Resources department or the Executive Director, as appropriate, for reports made pursuant to this policy and the investigation process.

15. The Executive Director will inform the Board of Directors at least annually of the number and type of privacy breaches and information incidents reported and corrective measures taken.

2.10.3 Requesting Correction of Personal Information

Scope:

This policy applies to employees who receive a request to correct the personal information of a current/former employees, Family Caregivers, Respite Family Caregivers, volunteers, or students requesting correction of their personal information.

Employees should refer to *3.1.21 Personnel Files* policy for requesting access to their employee information.

Students should refer to the *3.4.1 Practicum Student Program* policy for details on requesting access to their personal information stored at PLEA.

Participant requests to correct information will be handled as per their program's policies and procedures, in compliance with *Schedule F, Information Management (Records Privacy and Security)* of their funding contract.

This policy should be read in conjunction with:

- *1.5.2 Responding to Legal Action* policy
- *1.5.3 Confidentiality of Records* policy
- *2.10.0 Privacy Program Overview* policy
- *2.10.1 Personal Information Management* policy
    - *Appendix 2.10.1A Confidentiality Agreement*
- *2.10.2 Information Incident Management* policy
- *3.1.21 Personnel Files* policy
- *3.4.1 Practicum Student Program* policy

Statements:

1. The purpose of this policy is to clarify how PLEA supports individuals in exercising their rights to correct their personal information held by PLEA.

2. PLEA respects the rights of individuals to correct their personal information, where applicable.

3. PLEA does not correct third party information.

Procedures:

Requests to Correct Personal Information

1. Individuals may request correction to their personal information in order to ensure its accuracy and completeness.

2. Individuals who request to correct their personal information must do so in writing, using the *Appendix 2.10.4A Request to Correct Personal Information Form.*
    a. A request to correct personal information must provide sufficient detail to identify the personal information and the correction being sought.
    b. Requests to correct personal information must be sent to PLEA's Privacy Officer (privacy@plea.bc.ca).

3. Requests to correct information will be forwarded by the Privacy Officer to the party accountable for overseeing the personal information.

4. Within 30 business days of receiving a request to correct personal information, the party accountable for overseeing the personal information must:
    a. Correct any personal information discovered to be inaccurate or incomplete;
    b. If the information is corrected, make all reasonable efforts to provide a copy of the corrected personal information to any organizations in which the incorrect or incomplete information was disclosed within the past 12 months; or
    c. If no information is corrected, annotate the personal information to indicate that the correction was requested but not made.

Confidentiality

5. Requests for the correction of personal information are stored securely by the Human Resources department.

COMMUNITY SERVICES

2.10.4 Privacy Audits

Scope:

This policy applies to PLEA management.

Statements:

1. PLEA recognizes that the completion of privacy audits promotes awareness and understanding of the privacy implications associated with the agency's operations.

Definitions:

Privacy Audit: a process of reviewing the personal information a program/department is currently collecting, where it is stored and how it is managed. Privacy audits take an inventory of the program/department's existing records and information management practices and analyze how and why the program/department uses that information.

Procedures:

Privacy Audits

1. Directors are responsible for completing a privacy audit for their program/department every three years as part of their strategic planning; such audits should be reviewed in November of each year and updated as required. Privacy audits are completed using Appendix 2.10.4A *Privacy Audit Form*.

2. Completed audits are stored securely by the program's management and submitted every three years to the Privacy Officer (privacy@plea.bc.ca); submission dates align with the CARF surveying period. Completed privacy audits are made available to relevant stakeholders as required.

3. If the results of privacy audit indicate that improvements are needed to the program/department's personal information protection practices, the Director overseeing the program/department is responsible for leading and implementing those changes.

COMMUNITY SERVICES

CONFIDENTIALITY AGREEMENT

I, _____acknowledge that I understand that PLEA's privacy and confidentiality policies are available on the PLEA website and that I have been shown how to find them. I have also received a copy of PLEA privacy policies.

I understand that privacy and confidentiality matters are governed by BC and Canadian law, by obligations imposed on PLEA by contract, by ethical principles widely accepted in the human services and by PLEA's policies; and that violations could result in legal consequences in addition to action by PLEA.

I understand my duty to protect the personal information that I am responsible for and the confidentiality of the information that may come into my possession or be made available to me in my relationship with PLEA; to protect personal information against unauthorized access or disclosure; and to ensure the security of records and information.

I will not use or disclose such information except as authorized in order to discharge my duties to PLEA, or as required by law. I will follow the instructions that I receive from PLEA regarding personal and confidential information, including its return, retention and disposal. I will contact and consult with my supervisor (i.e., the person overseeing my involvement with PLEA) and/or PLEA's Privacy Officer when I need advice.

I understand the limits to my duty to protect personal information are as follows:

1. **Children in need of protection:** PLEA is required under the *Child, Family, and Community Service Act of British Columbia* to report instances where it has reasonable cause to believe a child is in need of protection to the appropriate authorities. I understand I am obligated to inform my supervisor or their designate immediately and follow their instructions in the following situations:
    a. Cases of suspected abuse or neglect of a child/children.
    b. Cases in which a PLEA participant (i.e., an individual receiving services from PLEA, whether a youth or adult) with a history of sexual abusing others may have access to minor children.

2. **Potentially suicidal/homicidal/dangerous participants:** PLEA has a duty to report when PLEA participants are a risk to themselves or others. I understand I must inform my supervisor or their designate if I become aware of a participant's actions or intentions that pose a risk to the life, health or security of themselves or others.

I understand that all media inquiries must be referred directly to the Manager of Communications & Development. I will not speak to the media, unless specifically delegated to do so. If any member of the

Charitable Registration
10781 0467 RR0001
bcgeu

media approaches me, I will report this as soon as possible to the Manager of Communications & Development or, in their absence, their designate.

Signature: _____ Date Signed: _____

Manager or Designate (For PLEA Community Services Society of BC):

Name: _____ Position: _____

Signature: _____ Date Signed: _____

plea COMMUNITY SERVICES

Appendix 2.10.4A Privacy Audit Form

Each program/department is expected to complete a privacy audit every three years (reviewed and refreshed annually) as part of its privacy obligations.

Personal Information: information about an identifiable individual, other than business contact information, that is recorded in any form.

The purpose of this audit is to determine:

- If the personal information being collected, used or disclosed is necessary to a particular function or operation.
- Who can see what, when, where, how and why.
- To identify where improvements can be made to the program's privacy practices.

This form is designed for use by the program/department's management team to guide their privacy audit. The completed form is confidentially stored by the program's management team and made available to relevant stakeholders as required. Explanations should be provided for each answer (i.e., not just a 'yes' or 'no' answer).

Team: **Date of Review:**

1. How do you collect personal information (e.g., forms, interviews, surveys)?

2. What are your purposes for collecting/using/disclosing personal information?

3. What are your methods of obtaining consent from individuals/notifying individuals of purpose of collection/use/disclosure? (verbal statements, paper or electronic notices etc.)

4. Does the program/department disclose personal information to anyone outside the program/department? If so, what stipulations are put into place to protect the personal information?

5. What are the safeguards in place to ensure personal information stays accurate and up-to-date?

Developed: November 2021—HR

6. Where/how does the program/department store personal information? (e.g., paper files, single cabinets, databases, audio files, video files etc.)

7. Who has access to the personal information held by the program/department? Please list their names and titles. Review if still needed for operations.

8. How long does the program/department retain personal information?

9. How does the program/department destroy or dispose of personal information?