Applegrove Privacy Policy

Approved October 21, 2009
Amended January 29, 2024

1. Policy Statement

Applegrove Community Complex (Applegrove) values the trust of those with whom we interact and work, and of our community, and recognizes that maintaining this trust requires that we be transparent and accountable in how the agency treats information that is shared with it. Applegrove recognizes that participants and volunteers provide and share personal and sensitive information with Applegrove and its staff in writing and verbally, including information provided about and by children. Applegrove is committed to respecting the privacy rights of all individuals by ensuring that their personal information is collected, used, disclosed and disposed of in an appropriate manner.

Applegrove is an agency of the City of Toronto and complies with all relevant provincial and municipal policies and laws. Applegrove's privacy policy is based on the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) 1990, as amended, and any applicable by-laws and policies of the City of Toronto. Applegrove is required to comply with MFIPPA. If anything in this policy is in conflict with MFIPPA or City policies, MFIPPA or City policy will prevail.

2. Purpose

The purpose of this policy is to foster trust by establishing clear accountabilities for the protection and use of personal information collected, used, disclosed and disposed by Applegrove.

3. Definitions

"Personal information" means recorded information about an identifiable individual. Examples include:

- home address, personal email address, home phone number, identification numbers e.g. Social Insurance Number
- personal emails, forms or correspondence between an individual and Applegrove
- ethnic origin, religion, age, gender, sexual orientation, marital status
- educational, medical, criminal or employment history
- personal financial transactions or financial information, including account numbers related to personal bank accounts, or credit cards and other payment mechanism, collected for the purpose of employment or the purchase of goods or services
- the individual's name when connected to any of the above
- Internet data, including identifiable data captured via Applegrove website "cookies"
- the personal opinions or views of the individual except if they relate to another individual
- the views or opinions of another person about the individual.

To qualify as personal information:

- it must be about an individual in a personal capacity
- it is reasonable to expect an individual may be identified if the information is disclosed.

As a general rule, information associated with an individual in a professional, business or official capacity is not personal information.

"Personnel" refers to the entire workforce of Applegrove, including employees and non-employees such as volunteers, placement students, trainees, staff seconded from other agencies, contractors, and consultants.

"Record" means any record of information however recorded, whether in printed form, on film or electronic, and includes correspondence, a memorandum, book, plan, map, diagram, picture, photo, film, sound recording, video, etc.

4. Application

This policy applies to all Applegrove personnel.

5. Roles and Responsibilities:

5.1 Executive Director

The Executive Director is responsible for overall privacy management, including but not limited to document security, access, and may delegate responsibility for implementation of privacy management to another member of the management team.

5.2 Management

All managers are responsible for ensuring that the employees under their supervision have completed privacy training and are following Applegrove's Privacy Policy, and that additional personnel under their supervision have been provided with privacy and awareness information and training that is adequate and applicable to their role within Applegrove.

5.3 Employees

All employees who will handle personal information are responsible for completing the City of Toronto Protection of Privacy training and maintaining information to those specifications.

5.4 Personnel

All personnel are responsible for:

- Being aware of their privacy responsibilities in executing their duties at Applegrove;
- Managing personal information accordingly and appropriately;
- Being responsible for privacy of Applegrove business information regardless of whether the technology used to manage the information is personally owned or Applegrove owned; and
- Following the Applegrove Breach of Privacy Protocol in the event of a potential breach of privacy.

6. General

Applegrove is responsible for securing, protecting and maintaining the privacy of any personal information under its control.

a) All Applegrove personnel share responsibility for the protection of personal information privacy and compliance with the roles and responsibilities identified in this policy.
b) Access to personal information will be restricted to those individuals who require access to personal information in order to perform their duties and where access is necessary for the administration of Applegrove business.
c) Measures will be taken to ensure the security of personal information, including but not limited to:
    - Controls on physical access to information
    - Controls on electronic access to information
    - Cybersecurity measures as outlined in the Applegrove IT & Cybersecurity Policy
d) All data collected by the agency shall be owned by Applegrove, excepting that relating to programming or services delivered in partnership with other organizations. In such cases the agency will establish a data agreement clarifying data collection, ownership, storage, use, archiving and destruction.
e) Contract employees and consultants will be required to comply with this policy as a condition of their contract agreement with Applegrove.
f) Applegrove will make information about its policies and procedures relating to the collection and management of personal information readily available.

7. Confidentiality Principles

7.1 Program Participants

a) Information about program participants will be considered confidential within the centre as a whole.
b) Information disclosed by program participants to personnel will be shared only with relevant program and administrative personnel on a need to know basis.
c) Relevant personnel includes Applegrove employees, volunteers, trainees, placement students, staff seconded from other agencies and the supervisors of trainees, placement students and seconded staff.
d) When Applegrove offers programming in partnership with other organizations, Applegrove expects the partner to share relevant information about program participants. Such information will be subject to this Privacy Policy. Relevant information collected by Applegrove will be shared with the partner organization in accordance with a mutually agreed data collection and privacy agreement.
e) In compliance with all relevant laws, Applegrove will report suspected child abuse or neglect, and provide all required information to appropriate authorities.

7.2 Personnel

a) Personal information about Applegrove personnel is confidential and will be shared only with relevant administrative staff, or in the case of the Executive Director, with

designated City of Toronto staff or Board members on a need to know basis for employment-related purposes.

8. Collection of Personal Information

8.1 Purposes

Applegrove will collect personal information about personnel, program participants, members and users of the agency in order to:

a) Maintain complete and accurate records with respect to:
   - program participants
   - agency members, for membership purposes
   - donors, sponsors and benefactors;
b) Maintain complete and accurate personnel files;
c) Communicate effectively with agency members and users, provide services and to communicate and work with third parties providing goods and services to those participants and programs;
d) Plan for, and to measure the quality, effectiveness and efficiency of programs
e) Solicit support from donors, sponsors, benefactors and volunteers, and to communicate effectively with such individuals; and
f) Comply with lawful requests from governmental agencies such as Canada Customs and Revenue Agency and the Ontario Human Rights Commission.

8.2 Form

Personal information will be collected on forms that include

a) The legal authority for the collection;
b) The principal purpose(s) for which the personal information is intended to be used; and
c) The title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection.

8.3 Consent

Any person collecting personal information on behalf of Applegrove must obtain consent from the individual from whom the information is being collected. If the individual is unable to provide consent (e.g. is a child) consent must be obtained from their legal representative (e.g. parent, guardian). An individual may withdraw consent at any time. Applegrove will inform the individual about any implications of withdrawal, if any.

8.4 Accuracy and Correction

Applegrove will make every reasonable effort to ensure that personal information collected will be as accurate, complete and up-to-date as possible for the purposes for which the information is to be used.

At least once annually, Applegrove will offer members the opportunity to correct their personal information. Upon request, members and program participants can correct their personal information at other times.

8.5 Access to Personal Information

An individual who provides personal information to Applegrove has the right to access the information and to ensure its accuracy and completeness. Applegrove will respond promptly to individuals' requests for access to their personal information. Access will be provided with advance notice during normal business hours by appointment.

An individual may correct errors or omissions and, if the information was shared with a third party within the prior 12 months, request that the third party be notified of the correction.

8.6 Disclosure

a) Among other exemptions, MFIPPA allows disclosure of personal information:
   - If the individual agrees;
   - In compelling circumstances affecting an individual's health and safety (if the individual is then notified by mail of the disclosure);
   - Under an Act of Ontario or Canada that authorizes the disclosure;
   - To a law enforcement agency to aid a law enforcement proceeding or from which a law enforcement proceeding is likely to result;
   - In compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased; or
   - To the Chair of the Management Board of the provincial cabinet or the provincial Information and Privacy Commissioner.

b) Prior to disclosure of personal information, the Executive Director, or designate, shall verify the requestor's identity and authority to request and receive the information.
c) Requests for disclosure from the police, the courts or other mandated bodies will be referred to the Executive Director or designate, and require their express permission before their release unless the request is received in the form of a subpoena. For all requests, only the specific information requested will be released.
d) Applegrove will maintain a complete record of third parties to whom personal information has been disclosed, and will make that record available to individuals whose personal information has been disclosed.

8.7 Disposition

Personal information will be made anonymous, or will be securely erased or destroyed in accordance with the Applegrove Records Retention Policy, when the information is no longer relevant or as permitted by law.

9. Breach of Privacy

Applegrove's Breach of Privacy Protocol will be followed in the event of any potential breach of privacy. See Appendix A.

Related Policies

Applegrove Records Retention Policy

Appendix A

Applegrove Breach of Privacy Protocol

May 2022
Updated January 2024

1. Purpose

The purpose of this protocol is to identify a privacy breach and to outline what action Applegrove Community Complex (Applegrove) must take when one occurs. All employees should follow this protocol.

2. Background

A privacy breach occurs when personal information is collected, used, disclosed and or destroyed in ways that are not in accordance with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) or the Personal Health Information Protection Act (PIPEDA), (the Acts).

The most common breach of personal information is the unauthorized disclosure of personal information contrary to section 32/31 of the Acts. Examples of breaches include a lost or misplaced file, a lost or stolen laptop, unauthorized access to personal information (electronic/hardcopy) or the inadvertent disclosure of personal information (e.g. human error in misdirecting a fax or e-mail).

Information will likely qualify as personal information if an individual can reasonably be identified from either the information alone, or from the information in combination with other information. Personal information may also include information that is not recorded (e.g., a verbal disclosure).

Personal information includes, but is not limited to:

- Name
- Personal address
- Personal email address
- Personal telephone number
- Race
- National origin
- Ethnic origin
- Skin colour
- Religion
- Age
- Date of birth

- Sex
- Sexual orientation
- Gender
- Marital status
- Family status
- Education
- Medical history
- Employment history
- Financial transactions involving the individual
- Identifying number
- Identifying symbol
- Photograph of the individual
- Other identifying particular
- Finger prints
- Blood type
- Correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature, or replies to the correspondence that would reveal the contents of the original correspondence
- The personal opinions or view of the individual except where they relate to another individual
- The views or personal opinions of another individual about the individual

3. Roles and Responsibilities:

All employees who will handle personal information are responsible for completing the City of Toronto Protection of Privacy training and maintaining information to those specifications.
All managers are responsible for ensuring that the employees under their supervision have completed privacy training and are following Applegrove's Privacy Policy.
The Executive Director is responsible for overall privacy management, including but not limited to document security, access, and may delegate responsibility for implementation of privacy management to another member of the management team.

4. Procedure

All employees, when faced with a potential privacy breach, will:

a) Identify the scope of the potential breach and take steps to contain it. Examples of containment measures include: deleting a social media post that inadvertently shows a photo of a child with their name and age; retrieving and securing documents that were disclosed and ensuring that no copies were made or retained by an unauthorized individual; changing a password known to an unauthorized individual; and shutting down a computer that has been hacked.

b) Report the incident to their supervisor, who must report to the Executive Director immediately.

The Executive Director will:

c) Immediately notify the appropriate staff within the City, including the Director, Corporate Access and Privacy Office (CAP) at 392-9683 / privacy@toronto.ca. In the event of a significant breach and/or as directed by the CAP, the Executive Director will also notify the Director of Community Resources, Social Development Finance and Administration division, and the City Clerk's Office.
d) Immediately isolate any physical or system resource that may contain evidence (e.g., paper files, workstations, logs, electronic records, e-mail files, etc.).
e) Keep existing back-ups (take tapes out of circulation) and back up any system resource associated with the incident.
f) Retrieve the hard copies of any personal information disclosed.
g) Ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required.
h) In consultation with the appropriate staff, determine whether the privacy breach could allow unauthorized access to any other personal information.
i) Document all actions (dates and times) taken during containment.
j) Determine if the response to the incident needs to be escalated (e.g., to a law enforcement agency).

4.1 Notice to Affected Parties

The City is also required under the Acts to provide notice to affected parties when a privacy breach occurs. This will be done by the City or by Applegrove and includes:

- Identifying those individuals whose privacy was breached and, barring exceptional circumstances (e.g. no known last address), notifying those individuals (e.g., by telephone or in writing).
- Providing details of the extent of the breach and the specifics of the personal information at issue and advise of the steps that have been taken to address the breach, both immediate and long-term.

4.2 Investigation

The City may conduct an internal investigation of the privacy breach and:

- Inform the Information and Privacy Commissioner/Ontario (IPC/O) Registrar of the privacy breach and advise of immediate containment and notification actions taken.
- In consultation with the IPC and program staff, conduct an internal investigation into the matter. The objectives of the investigation are to ensure the immediate requirements of containment and notification have been addressed; review the circumstances surrounding the breach; review the adequacy of existing policies and procedures in protecting personal information and implement changes to prevent future breaches.

- Advise the IPC/O in writing of findings and work together with program staff and the IPC to make necessary changes.

The IPC may issue a report with additional recommendations.

4.3 Resolution/Remedies

The Executive Director in consultation with City staff and IPC/O will identify resolutions/remedies. Applegrove is expected to:

- Implement City and IPC recommendations (e.g. revising and or developing policies, procedures).
- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of the Acts.

4.4 Sample Situations and Responses

A promotional email is inadvertently sent out to 200 people using “cc” instead of “bcc”.
Actions:

- Inform recipients that recipient e-mail addresses were inadvertently disclosed and apologize for the error.
- Ask recipients to delete said e-mail (both from their inbox and trash).
- Provide the Executive Director’s contact information should anyone have any questions.
- Employee responsible to review the City of Toronto Secure Use of Email Guidelines.
- Executive Director to notify the Corporate Access and Privacy Office and implement any additional recommended actions.

A photo of a child for whom Applegrove does not have photo consent is posted on the Applegrove Instagram feed.
Actions:

- Delete the post as soon as the error is identified.
- Notify your manager and provide details (child’s name, when posted, how long, etc.).
- Manager informs the child’s parent/guardian of the breach and steps taken. Provides Executive Director contact information should there be further questions or concerns.
- Executive Director to notify the Corporate Access and Privacy Office and implement any additional recommended actions.
- Management and employee review process for photo consent, storage and selection to identify potential contributors to the error and steps to prevent it from happening again.