Elections Ontario

Elections Ontario Privacy Policy

Office of the Chief Electoral Officer
Elections Ontario
January 2021

Document History

Revision Number	Revision Date	Effective Date	Description of Changes	Approved By
1.2	December 8, 2020	January 6, 2021	• Merged with Privacy Program Terms of Reference • Clarified sources of privacy guidance used • Updated definitions • Updated principles 1 to 5, 9 • Clarified escalation processes, enforcement, training, and responsibilities	Chief Electoral Officer
1.1	February 4, 2013	February 4, 2013	Correction of typographical error	Chief Privacy Officer
1.0	November 7, 2012	November 7, 2012	Original	Chief Electoral Officer

Merged: Privacy Program Terms of Reference

Revision Number	Revision Date	Effective Date	Description of Changes	Approved By
1.1	February 4, 2013	February 4, 2013	Correction of typographical error	Chief Privacy Officer
1.0	November 7, 2012	November 7, 2012	Original	Chief Electoral Officer

TABLE OF CONTENTS

Section 1: Introduction

Elections Ontario (EO) is responsible for managing, administering, and overseeing the electoral process for Ontario under the direction of the Chief Electoral Officer (CEO). As part of its work, EO has been entrusted with the personal information (PI) of Ontario electors and future voters, political entities, the public, and employees. Protecting the privacy of this information is an integral part of the organization's business operations.

The Elections Ontario Privacy Policy provides the overarching privacy framework for EO. It applies to all EO employees, contractors and sub-contractors, and other agents. Its primary purpose is to set out the ways in which EO can collect, use, and disclose PI, in a manner that is transparent to both internal and external stakeholders.

A secondary purpose is to set out roles and responsibilities of EO's agents for strategic and operational aspects of the privacy program; EO employs a decentralized governance framework in which the Chief Privacy Officer (CPO) has been delegated responsibility for privacy operations, and is supported by subject matter experts (SMEs) within the Privacy Office.

This policy applies to all EO employees, contractors and sub-contractors, and other agents. For greater certainty, this policy applies to all field staff, including Returning Officers (ROs) and Election Clerks (ECs).

The CPO owns this policy, and expertise is provided by EO's Privacy Office. Questions about this policy can be directed to priv@elections.on.ca.

Section 2: Principles

Data protection is a shared responsibility. True accountability is only possible when all EO personnel understand the role that they play in ensuring the success of the program.

In implementing its privacy program, EO will:

- Respect the privacy of individuals whose PI is collected, used, and disclosed by EO.
- Reduce individual and organizational risk through continued efforts to improve EO's privacy policies, procedures, and training.
- Integrate privacy best practices into business practices and the design of programs, services, systems, and processes at EO.

EO recognizes the definition of PI set out in Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA).

EO manages and protects its PI in accordance with the 10 Canadian Standards Association (CSA) model code principles. These principles are reflected in Canadian and Ontario privacy laws, and in the privacy laws of other jurisdictions.

EO adheres to the requirements set out in the *Election Act* and *Election Finances Act*, as well as other applicable laws, respecting PI. EO also adheres to information sharing agreement (ISA) requirements from its data partners, as well as information security requirements from third parties and vendors that work with EO. Finally, EO adheres to the privacy best practices set out by the Information and Privacy Commissioner of Ontario (IPC), the Office of the Privacy Commissioner of Canada, and other authoritative sources of guidance both nationally and internationally.

In the event of any changes to legal and regulatory guidance, or changes to EO's operations that affect how it collects, uses, discloses, retains, and/or disposes of PI, this policy should be revisited.

A copy of this policy is provided to all EO headquarters (EOHQ) employees and key staff when they are onboarded, and a summary of key privacy considerations is provided to poll officials. A copy is also made available to the public through EO's website (www.electionsontario.on.ca).

Section 3: Scope

This policy provides guidelines for the protection of the PI in the custody and under the control of EO, in any medium. These include:

- Elector information, contained in the Permanent Register of Electors for Ontario (PREO), Absentee Register, and the Ontario Register of Future Voters (ORFV); list products; as well as eRegistration requests and special ballot applications. It may also include additional information collected from electors in the course of research, such as through surveys.
- Political entity information, contained in financial filings, lists of contributors over $100, and registration information of political entities associated with the *Election Finances Act* and the *Taxpayer Protection Act, 1999;* information contained in the candidate nomination papers, and information about scrutineers, as set out in the *Election Act*; and information related to investigations and complaints made under the *Election Finances Act* and the *Election Act*. Some documents are public records according to Section 15(1) of the *Election Finances Act*. As such, not all privacy considerations around collection, use, disclosure, accuracy, retention, and safeguards will apply to these records. Political entity information also includes research data collected from political entities, such as members of the Political Advisory Committee.
- Stakeholder information, contained in formal complaints and investigations under the *Election Act* or *Election Finances Act*; as well as questions related to electoral processes, website feedback, billing information, mailing lists, research data, and video and audio recordings.
- Employee information, contained in resumes, onboarding and termination forms, performance evaluations, research data, and video and audio recordings. For greater certainty, this category of information includes information about job applicants, current employees, and former employees.

This Privacy Policy does not address EO's use of web analytics information, which is more fully dealt with in EO's web Terms of Use (https://www.elections.on.ca/en/terms-of-use.html)[1].

[1] Though out of scope, it is recommended that EO's web Terms of Use be revisited for accuracy in 2021, to ensure that it continues to accurately reflect EO's vendors for web analytics and the identifying nature of the information that is collected.

Section 4: Definitions

The following definitions are referred to throughout this policy:

Absentee Register:

A register of electors who are temporarily resident outside Ontario but entitled to vote in an electoral district in Ontario.

Chief Privacy Officer:

The designated EO executive responsible for managing and overseeing EO's privacy operations.

Confidential Information:

Information that may negatively impact EO if it were to be made known to unauthorized individuals. This can include PI as well as other, non-personally identifying information such as plans, internal reports, contracts and agreements, proprietary information, and information relating to the security configuration of any of EO's IT systems.

Elector:

A person who is a Canadian citizen at least eighteen years old, and who meets the residency criteria for Ontario. Also known as an eligible voter.

Elector Information:

PI about Ontario electors and prospective electors.

Election Finances Information:

Documents filed with the CEO under Section 15(1) of the *Election Finances Act*. These are public records and include registration documents and financial statements.

Electoral Products:

Products produced during and outside an electoral event that contains elector information that is derived from the PREO and/or Absentee Register.

Electoral Purposes:

For administering elections, by-elections, or referenda, including communicating with electors, soliciting contributions and campaign

support, and conducting research (including analysis and data visualization) to improve the administration of elections.

Employee Information:

Information about job applicants, current employees, and former employees of EO, as well as ROs.

EO Personnel:

EO personnel include employees involved in administering or managing any EO program area. This includes individuals retained by EO to manage the electoral process during general elections and by-elections (e.g. ROs, key staff, poll officials, etc.).

Express Consent:

Consent that has been clearly given, either orally or in writing.

Geographical Products:

A type of electoral product. All maps and polling division information provided during an electoral event. Geographical products do not include PI, although PI is used by EO to generate the products.

Implied Consent:

Consent that one concludes has been given, based on an individual's action or inaction in the circumstances.

Key Staff:

Individuals hired to work either in a returning office or satellite office.

List Products:

A type of electoral product. Any list containing elector information, such as the annual update to PREO and the Absentee Register, lists of electors provided to political entities at the end of each calendar year, and lists of electors provided at the beginning of each event. List products generally include elector name, their unique identifier, residential address, and mailing address. A full description of list products can be found in EO's Guidelines for the Use of Electoral Products.

Ontario Register of Future Voters (ORFV):

A provisional register of persons who are 16 or 17 years of age, are Canadian citizens and who reside in Ontario. Records from the ORFV are

transferred to PREO when the person reaches 18 years of age, or when the CEO is aware that the person will be 18 during the election period.

Permanent Register of Electors for Ontario (PREO):

An up-to-date database of eligible Ontario voters. PREO contains the elector's name, address, and date of birth.

Personal Information:

Personal identifiable information about any individual, such as name, home address, home/cell phone number, personal email address, date of birth, social insurance number, some voting information, and financial information. It also includes personally identifiable information about EO personnel or service providers (e.g. about employees' education, health or employment history). PI can include any identifying number, symbol or other particular assigned to the individual. PI does not include business contact information. EO refers to the definition of PI set out in Ontario's *Freedom of Information and Protection of Privacy Act*, Section 2(1).

Political Entities:

For the purposes of this policy, "political entities" include political parties, constituency associations, nomination contestants, candidates, leadership contestants, and third parties (as defined in the *Election Finances Act*) that are registered or undergoing registration; as well as registered campaign organizers. These parties are further described under the *Election Finances Act* and the *Taxpayer Protection Act, 1999*.

Political Entity Information:

PI about political entities (specifically, individuals listed on registration forms).

Poll Official:

An individual hired to work at a poll either during the advance polls or on polling day for the purpose of supporting the voting process.

Privacy Office:

A decentralized body of executives, directors, managers, and subject matter experts (SMEs) comprising the CPO and those who support the implementation of privacy programming at EO. The Privacy Office is an

oversight group responsible for advising on matters such as breach management, privacy issues and risks, and privacy opportunities.

Public:

All members of the public, who may or may not be electors.

Service Provider/Vendor:

Companies or individuals (third parties) that collect or retain PI for EO or are provided PI by EO to perform their services.

Stakeholder Information:

PI about members of the public.

Section 5: Mandatory Requirements

This section describes EO's requirements related to PI in its custody and control, using the CSA model code as a guiding framework.

5.1 Principle 1: Accountability

5.1.1 Principle 1 states: "An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the privacy principles."

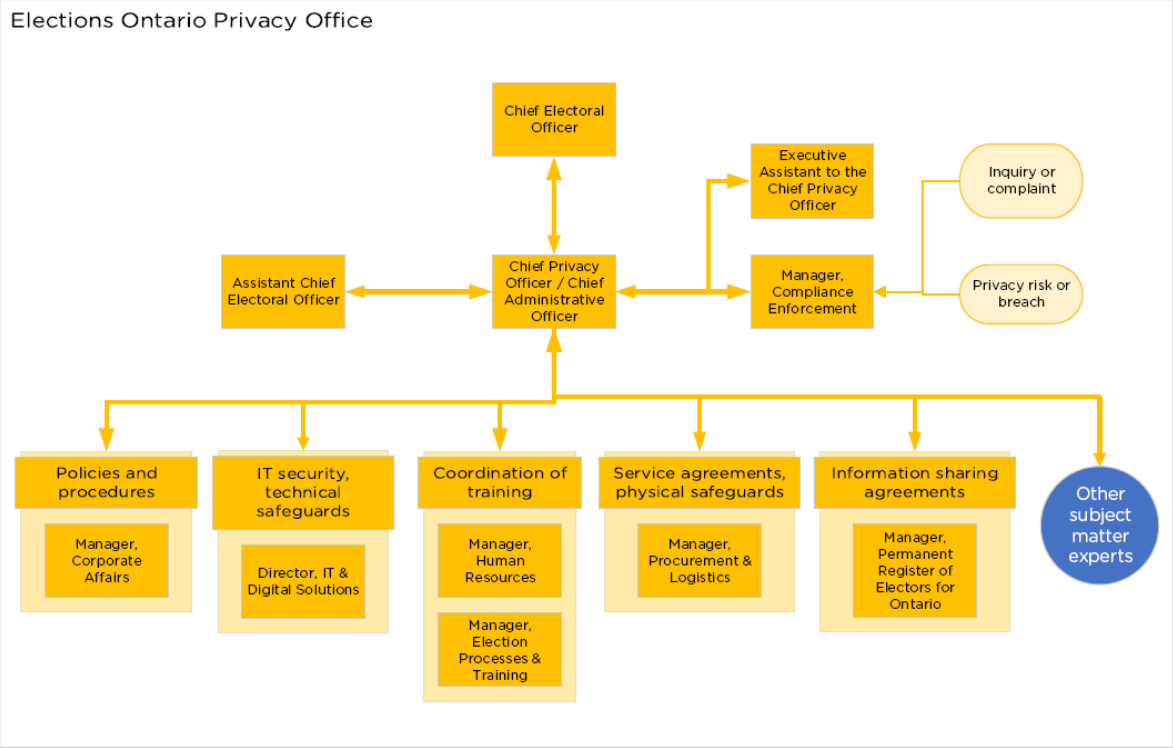
5.1.2 EO is responsible for ensuring the protection of PI that is in its custody or control.

5.1.3 The following roles are central to EO's privacy governance framework, which helps to facilitate the protection of PI:

- The Chief Electoral Officer (CEO), an independent officer of the Legislative Assembly, is ultimately responsible for the protection of PI in the custody or control of EO.
- The CEO has delegated responsibility for the oversight and management of EO's privacy operations to the CPO. The CPO will communicate program updates to the CEO. The CPO will also communicate relevant issues and concerns to the Assistant Chief Electoral Officer (ACEO) where it relates to their cluster.
- The CPO is a part of and is supported by other members of the Privacy Office, a decentralized network of privacy champions who are responsible for ensuring that robust control measures are in place to ensure privacy and security of PI. Members are drawn from various divisions at EO. On an ad-hoc basis, other SMEs, such as data stewards or the business owners of specific agreements addressing PI, can also be added to the Privacy Office structure. See Figure 1 for details.
- Within the Privacy Office, the Manager, Compliance Enforcement is primarily responsible for facilitating intake of inquiries, complaints, risks, and breaches; and the Executive Assistant to the CPO acts as their backup for this activity.

The below figure illustrates EO's governance framework at a high level, and the respective roles of each member of the Privacy Office[2]. Arrows represent key lines of communication.

Figure 1: Elections Ontario Privacy Office



5.1.4 Privacy is inherently interdisciplinary, and a rapid response is often required to address time-sensitive risks and issues. It is expected that members of the Privacy Office will provide timely assistance to the CPO, balancing their privacy responsibilities with their day-to-day work.

5.1.5 EO requires all its employees, contractors and sub-contractors, and agents to meet the privacy requirements and responsibilities set forth in this policy. All EO personnel and service providers are

[2] At the time of this writing, records management does not have a designated lead. EO will continue to adhere to existing records management policies and procedures until its records management program is revisited.

responsible for understanding EO's privacy and security policies and procedures, reporting privacy risks and breaches, and participating in privacy programming, which may include self-audits, breach investigations, and training.

5.2 Principle 2: Identifying Purposes

5.2.1 Principle 2 states: "The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."

5.2.2 Elector Information: EO uses identifiable information about electors, such as name, residential address, mailing address, date of birth, and limited financial information, for the following purposes:

- To establish and maintain voting registers under Sections 17.1(1), 17.7(1), and 45.13(1) of the *Election Act*, including PREO, the Absentee Register, and ORFV; and to verify the accuracy of PREO, in accordance with Section 17.1(2) of the *Election Act*.
- To establish and maintain an electronic system (eRegistration) to allow electors to verify and confirm information about themselves in PREO, in accordance with Section 17.1.1(1) of the *Election Act*.
- To generate electoral products that are shared with employees, political entities, and members of the public under the *Election Act*. See EO's Guidelines for the Use of Electoral Products for details.
- To generate internal reports containing PI for operational purposes.
- To calculate aggregate statistics related to elections, such as the number of electors that were entitled to vote in a given election, as set out under Section 64 of the *Election Act*.
- To facilitate research activities that help EO to improve the administration of elections, by better understanding event-related issues, risks, and opportunities for process improvement.

5.2.3 Political Entity Information: EO uses PI about political entities, such as such as financial filings, lists of contributors over $100, and registration information of political entities associated with the

Election Finances Act and the *Taxpayer Protection Act, 1999*; information contained in the candidate nomination papers, and information about scrutineers, as set out in the *Election Act*; and information related to investigations and complaints made under the *Election Finances Act* and the *Election Act*, to:

- Facilitate public inspection of candidate nomination papers and election finances information.
- Address compliance issues identified during the compliance review processes associated with financial filings.
- Address orders and complaints made under the *Election Act* and the *Election Finances Act*, and to enforce compliance with these acts.
- Investigate election documents for possible corrupt practices in accordance with Section 86(2) of the *Election Act.*

EO also collects and uses political entity information for research purposes, to improve the administration of elections.

5.2.4 Stakeholder Information: EO collects information from the public, including name, contact information, and billing information, for the following purposes:

- To address complaints and investigations under the *Election Act* or *Election Finances Act.*
- To respond to questions about the electoral process.
- To improve EO's website.
- To fulfill map orders and educational resource orders.
- To conduct research involving the public, to gain a better understanding of their experiences interacting with EO's products and services and to improve these products and services; and to facilitate research honorariums.
- To generate mailing lists for communicating elections-related news.
- To facilitate security of EO buildings, persons on-site, and/or IT systems (e.g. when EO collects video and audio recordings at its offices in order to investigate building security incidents, or when it tracks IP addresses in order to detect malicious activity on its websites).

5.2.5 Employee Information: EO collects, uses, and discloses PI about employees and ROs including name, address, date of birth, social insurance number (SIN), gender, telephone number and email address, employment and education history, medical information and workplace accommodations, citizenship status, bank account information, benefits and pension information, performance evaluations and attendance information; as well as name, address, telephone number and email address, and employment and education history of job applicants; for the following purposes:

- To determine eligibility for employment, including verifying qualifications and references.
- To perform background checks (criminal record and judicial matters checks) on specific roles requiring greater clearance, such as ROs and ECs.
- To communicate with the individual for work-related purposes.
- To communicate with the individual's emergency contacts if they are injured or fail to show up at work.
- To establish training and development requirements, and track training completion.
- To assess performance and manage performance issues if they arise.
- To administer pay and benefits.
- To manage attendance and leaves.
- To facilitate workplace accommodations.
- To process employee work-related claims (e.g. benefits, workers' compensation, insurance claims).
- To comply with applicable laws (e.g. Canada's *Income Tax Act*; Ontario's Human Rights Code; *Employment Standards Act, 2000*; *Occupational Health and Safety Act, 1990*; *Election Finances Act*).
- (For ROs only) To communicate about elections-related issues during and in between election events, to inform orders in council (OICs), and to ensure consistency between names in OICs and writs.

In addition to the above purposes related to establishing, maintaining, and terminating the employment relationship:

- EO collects and uses PI related to staff for the purpose of understanding their perception of training and work, such as through focus groups and surveys.
- EO collects and uses PI related to field staff who had worked at previous events to facilitate recruitment for future events.
- EO collects and uses PI related to staff in the form of video and audio recordings at its offices, to investigate building security incidents. Information is captured in public areas as well as some work areas.
- EO discloses PI to third parties to facilitate work references, with the express consent of the employee or former employee to which the information relates.
- EO discloses PI related to field staff to other Canadian electoral agencies to assist them with event employment recruitment.

5.3 Principle 3: Consent

5.3.1 Principle 3 states: "The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate."

5.3.2 In general, EO will obtain express consent when collecting PI, where the PI involved is sensitive, where the purpose of the collection is not reasonably foreseeable, or where there is a substantial risk of significant harm even after all mitigation activities have been taken. Express consent is obtained prior to or at the point of collecting the information. In other instances, implied consent may be used.

5.3.3 Elector Information: EO collects PI about electors and prospective electors ages 16 or 17 in Ontario without consent in order to establish and maintain its registers, to verify the accuracy of PREO, to establish and maintain an electronic system for verifying and confirming PREO information, to prepare electoral products, and for electoral purposes as set out in the *Election Act*. EO can collect elector information indirectly from authorized governmental agencies (e.g. the Ministry of Transportation), the Chief Electoral

Officer of Elections Canada, and other sources the CEO considers reliable, pursuant to Section 17.1(4) of the *Election Act*.

When electors request to vote by mail, EO requests express consent before sharing any of the special ballot application information with its data partners and/or updating PREO with the information.

5.3.4 Political Entity Information: EO collects PI without consent from political entities in accordance with the *Election Act*, the *Election Finances Act*, and the *Taxpayer Protection Act, 1999*. Where EO collects PI from political entities for research purposes, it does so in accordance with the principles set out in 5.3.2 and 5.3.7.

5.3.5 Stakeholder Information: EO collects PI with consent from members of the public through its general inquiries and complaints process, and through web forms. In general, PI will only be collected directly from the individual to whom it relates. Emails associated with EO's mailing lists clearly identify the sender and include an option to unsubscribe.

5.3.6 Employee Information: EO collects PI without consent only for the purposes of establishing, managing, or terminating the employment relationship, and for addressing building security incidents. EO collects PI with consent for purposes unrelated to the employment relationship, such as to provide a reference to a third party, to understand their perceptions of training and work, and to provide their information to other electoral agencies for recruitment purposes. In general, express consent is obtained.

5.3.7 Where PI is collected without consent, a notice of collection will still be provided prior to or at the point of collection whenever feasible and practical. Such notice will include a reference to EO's legal authority for the collection, the purpose(s) for which the PI is intended to be used; and the title, business address and business telephone number of an individual who can answer questions about the specific collection.

5.4 Principle 4: Limiting Collection

5.4.1 Principle 4 states: "The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means."

5.4.2 EO only collects PI for purposes set out under Principle 2. Unsolicited PI is securely deleted from EO systems as soon as possible.

5.4.3 EO implements administrative controls (e.g. forms and call center processes) and technical controls (e.g. field mapping during data processing) to ensure that it does not collect any more PI than necessary for its relevant programs or activities.

5.4.4 PI is collected directly from the individual to whom the information relates whenever it is feasible and practical to do so. Direct means of collecting PI include but are not limited to:

- Requesting PI from electors through the eRegistration application, at a returning office, or at a polling location.
- Requesting PI from political candidates via their nomination paper.
- Requesting PI from stakeholders to return their call regarding an elections-related inquiry or to respond to their complaint.
- Requesting PI from job applicants through a job posting and requesting additional PI during the onboarding process to set up the employee's account and payroll.

5.4.5 PI may be collected indirectly under limited circumstances, such as:

- When EO maintains its registers using information from Elections Canada and other reliable sources, as set out in Section 17.1(4) of the *Election Act*.
- When EO surveils its own office premises through closed-circuit television (CCTV) or microphone recordings.
- When EO gathers limited geographic information about members of the public as they browse EO's website.

- When EO takes video or audio recordings of focus group attendees or makes observations about the attendees' demographic characteristics.

In all such events, the individuals to whom the PI relates will receive a notice of collection. If this information is unclear or missing, individuals are advised to reach out to priv@elections.on.ca.

5.5 Principle 5: Limiting Use, Disclosure, and Retention

5.5.1 Principle 5 states: "Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes."

5.5.2 Elector Information:

- EO uses elector information for electoral purposes, to generate electoral products, and to generate internal reports and aggregate statistics related to elections, in accordance with the *Election Act*. EO expressly prohibits the commercial use of elector information, in keeping with Section 17.4(1)(b) of the *Election Act*.
- Internally, EO shares PREO PI to facilitate research activities. Research may involve linking PREO data to other individual-level and aggregate information held by EO to generate additional insights about the elector's journey. This sharing is governed by internal memoranda of understanding, which set out the purpose and nature of the information being shared.
- EO discloses PREO PI for purposes permitted under the *Election Act*. First, the CEO may provide information contained in PREO to the Chief Electoral Officer of Canada and any municipality in Ontario and its local boards, for electoral purposes and in accordance with applicable laws, in accordance with Section 17.2 of the *Election Act*. These disclosures are governed by ISAs with the respective data partners, which include terms and conditions intended to limit the use and disclosure of the information, and to safeguard the information at rest and in transit. Second, political entities may request list products for electoral purposes. To do

so, they must provide EO with an acceptable Privacy Policy and otherwise adhere to EO's Guidelines for the Use of Electoral Products.

5.5.3 Political Entity Information:

- EO uses the PI collected in connection with the *Election Act*, *Election Finances Act*, and *Taxpayer Protection Act, 1999* to facilitate public inspection of candidate nomination papers and election finances information; to address compliance issues identified during the compliance review processes associated with financial filings; to address orders and complaints made under the *Election Act* and the *Election Finances Act*, and to enforce compliance with these acts; and to investigate election documents for possible corrupt practices.
- EO uses other political entity information collected through research to improve the administration of elections.
- Internally, EO shares candidate nomination papers among field staff for the relevant electoral district and EOHQ staff, to enable public inspection under Section 27.4 of the *Election Act*. It also shares election finances information amongst its Compliance staff to enforce compliance with the *Election Finances Act*.
- EO discloses filings made under the *Election Finances Act* to the chief financial officer and auditor of the relevant political entities as required.
- EO makes political entity information available to the public. See Principle 9 for more information about this process. However, in keeping with Section 2(3) of the *Election Finances Act*, the addresses of contributors shall not be published under certain circumstances.

5.5.4 Stakeholder Information: EO uses the PI to address complaints and investigations under the *Election Act* or *Election Finances Act*, respond to questions about the electoral process, improve its website, fulfill map orders and educational resource orders, conduct research and facilitate research honorariums, generate mailing lists, and investigate building and information security incidents.

- The information is shared internally with EO personnel who require it for consistent purposes.

5.5.5 Employee Information: EO uses the PI to establish, manage, and terminate the employment relationship; to understand perceptions of training and work; to facilitate recruitment; to investigate building security incidents; and to provide work references.

- Internally, EO shares the information among EOHQ staff who require it for consistent purposes, such as to assess performance and make decisions regarding termination, to facilitate training, to process payroll, to install workplace accommodations, and to help ROs recruit field staff for an event.
- EO discloses employee information to the Legislative Assembly of Ontario in order to facilitate processing of payroll. EO also discloses work references to third parties with the express consent of the individual to whom the information relates.

5.5.6 EO will limit internal data sharing to those individuals who require access to the information for their work and as permitted by EO's legal and agreement requirements. Principles of least privilege and need to know are followed. Access to PI is further addressed in EO's IT Access Control and User Access Management Policy. Relevant data stewards are responsible for ensuring that any privacy commitments made at the point of collecting the information are communicated to end users.

5.5.7 EO will only retain PI for as long as necessary to satisfy the purpose for which it was collected, as authorized by law, and in accordance with EO's Recordkeeping Policy and Records Retention Schedule. PI that is no longer required will be securely destroyed in accordance with EO's Personal Information Use and Retention Procedure.

5.5.8 From time to time, EO may receive requests for information from law enforcement. These will be handled according to Appendix A.

5.6 Principle 6: Accuracy

5.6.1 Principle 6 states: "Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."

5.6.2 EO is committed to ensuring that PI in its custody or control is as accurate, complete, and up to date as possible to meet the purposes for which the information was collected. It does so by:

- Enabling electors and future electors to add, update, or confirm their PI through eRegistration.
- Conducting targeted registration programs, in accordance with Section 17.14 of the *Election Act*.
- Enabling employees to review and update their PI through an online portal and/or by reaching out to Human Resources or Finance.

5.6.3 EO relies upon individuals to provide notification if there is a change to their PI, or if there is an error in the PI. See Principle 9 for more information about individual access procedures.

5.6.4 Where EO receives a request to correct the PI, and a decision is made not to apply the correction, it will retain this complaint with the record of PI.

5.6.5 Where EO receives a request to correct the PI, and a decision is made to apply the correction, a reasonable effort will be made by the line of business that owns the PI to notify any third parties in receipt of the PI.

5.7 Principle 7: Safeguards

5.7.1 Principle 7 states: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."

5.7.2 EO makes every reasonable effort to prevent any loss, misuse, disclosure, or modification of PI, as well as any unauthorized access to this information. Safeguards employed are based on the sensitivity of the information.

5.7.3 EO ascribes to privacy by design principles and makes an effort to ensure that privacy-protective designs are considered in the initial stages of building IT solutions involving PI.

5.7.4 In terms of administrative safeguards, the CEO has delegated responsibility for EO's privacy operations to the CPO, who is supported by the Privacy Office. Through this policy and through the

Privacy and Security Breach Management Protocol, EO has defined escalation processes for privacy inquiries, complaints, risks, and breaches that are flagged during and outside of events. EO personnel are provided with privacy and security policies and procedures at the point of being onboarded and attend privacy and security training[3]. Contractors and subcontractors that handle PI on EO's behalf are also bound by privacy requirements that are set out in their agreements with EO and in EO's policies and procedures.

5.7.5 In terms of technical safeguards, EO employs varied safeguards such as strong passwords, security logging, encryption, restricting access to USB ports on EO-issued laptops, and role-based access controls for information systems from which PI may be accessed.

5.7.6 In terms of physical safeguards, EO employs varied safeguards such as locking filing cabinets and rooms, ensuring clean desks, restricting physical access to its offices, and securely shredding paper records that are no longer needed.

5.8 Principle 8: Openness

5.8.1 Principle 8 states: "An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."

5.8.2 EO makes its privacy policies and practices publicly available through its website.

5.8.3 In addition, EO provides multiple channels for the public to ask questions and make complaints regarding its privacy practices, including priv@elections.on.ca and EO's general contact (info@elections.on.ca, 1-888-668-8683, or (TTY) 1-888-292-2312).

[3] As of this writing, EO's privacy and security training requirements for headquarters and the field are being revisited.

5.9 Principle 9: Individual Access

5.9.1 Principle 9 states: "Upon request, an individual shall be informed of the existence, use and disclosure of his/her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."

5.9.2 This policy provides information about the existence, use, and disclosure of certain types of PI. Using this information, an individual can make a request to access their own information. Although EO is not subject to FIPPA or the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), EO will provide access to individuals' own PI to the extent possible.

5.9.3 In certain situations, EO may not be able to provide access to all the PI it holds about an individual, due to considerations such as cost, legal requirements, security requirements, or commercial proprietary reasons; or if the record includes the PI of other individuals. Exceptions will be explained to the individual upon request.

5.9.4 Elector Information: Electors and future electors can access their own PI via eRegistration, an online portal where they can view, confirm, and modify their information. They can also make their request by emailing register@elections.on.ca, or by mail at:

Elections Ontario

Attn: PREO

51 Rolark Drive

Toronto, ON M1R 3B1

Individuals cannot opt out of the collection of their PI for the purposes of managing the electoral process. However, individuals can request that their information be removed or corrected on the voters list or ORFV through eRegistration or through the manual process.

5.9.5 Political Entity Information and Stakeholder Information: All EO stakeholders have the right to request access to their own PI if it is held by EO. Requests can be made by emailing priv@elections.on.ca.

In addition, all members of the public are permitted to publicly inspect the following documents:

- **Candidate nomination papers**: Nomination papers are made available for public inspection (1) at EO's office until the writ is issued, (2) at the office of the RO between the issuance of the writ and the return of the writ, and (3) at EO's office for one year after the return of the writ for the election, in accordance with Section 27.4 of the *Election Act*. Inspections are only available by appointment. Those interested may contact info@elections.on.ca or 1-888-668-8683 to request an appointment. Visitors must specify the nominations they would like to view and are not allowed to transcribe any information during their visit. All visitors will be escorted onsite per EO policy.
- **Election finances documents**: All documents that are submitted by political entities are available for public inspection at EO's office during normal office hours. Those interested may contact electfin@elections.on.ca or 1-866-566-9066 to request to review these documents.

5.9.6 **Employee Information**: Employees have the right of access to their own PI contained within their EO employee file.

- Current HQ employees may correct certain PI (e.g. address, personal contact information) via AIMS, and may request additional information by contacting the Manager, Human Resources.

- During an event, key staff can review and update their information using the Elections Management System (EMS), Human Resources Information System (HRIS) module. Poll officials can contact the relevant RO office or fill out an employee form on the Election Official Employment Centre[4]. Outside of

[4] Elections Ontario. (N.d.). *Election Official Contact Form.* https://www.elections.on.ca/en/about-us/employment-centre/election-official-employment-centre/election-official-contact-form.html

events, field employees can fill out an employee form on the Election Official Employment Centre.

- Former employees are requested to contact info@elections.on.ca or 1-888-668-8683 for assistance.

5.9.7 Prior to fulfilling a request, requestors may be asked to provide additional detail to help locate the record, including their name, address, contact information, and a description of the records that they are seeking and/or time period of interest.

5.9.8 Requests for PI on behalf of another individual will be considered on a case-by-case basis. Additional documentation may be required to support the request.

5.10 Principle 10: Challenging Compliance

5.10.1 Principle 10 states: "An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance."

5.10.2 Any individual may submit a concern or complaint regarding EO's privacy practices to the CPO by contacting priv@elections.on.ca. Further details are provided in Section 5.11, "Escalation Processes".

5.10.3 EO extends whistleblower protection to all employees. Employees will not face reprisal simply for reporting a concern or complaint regarding EO privacy practices.

5.11 Escalation Processes

5.11.1 Privacy inquiries and complaints, including requests for individual access to PI, should be directed to priv@elections.on.ca. The Manager, Compliance Enforcement, will monitor this email at least daily.

5.11.2 Immediately upon becoming aware of the privacy inquiry or complaint, the Manager, Compliance Enforcement will notify the CPO and the Executive Assistant to the CPO, who may provide additional feedback or direction.

5.11.3 Within two business days, the Manager, Compliance Enforcement will acknowledge receipt of the inquiry or complaint by responding to the sender.

5.11.4 The Manager, Compliance Enforcement and CPO will attempt to answer the question or resolve the issue. The Manager, Corporate Affairs, can be consulted if the issue relates to the interpretation of EO's privacy and security policies or procedures. The CPO may also request input from other members of the Privacy Office to draft an appropriate response.

5.11.5 The CPO may escalate inquiries and complaints to the CEO for their awareness and response.

5.11.6 The Manager, Compliance Enforcement is responsible for ensuring that all inquiries and complaints materials are centrally logged, and that records are retained in accordance with EO's Records Retention Schedule. The log of inquiries and complaints shall include the following information:

- Date received.
- Full name of the submitter.
- Full name of the individual(s) the complaint was against.
- Details of the actions taken, and any rationales for actions not taken, such as lack of jurisdiction.

5.11.7 The Manager, Compliance Enforcement is responsible for tracking the timeline for inquiry and complaint responses and following up with appropriate stakeholders. This includes facilitating communication with the inquirer in the event of any delays, refusals, or exemptions.

5.11.8 At any point, if the issue presents a privacy risk or breach, all stakeholders must follow EO's Privacy and Security Breach Management Protocol, in addition to any other instructions provided.

5.12 Training

5.12.1 The CPO, in collaboration with Corporate Affairs, Human Resources, and Election Processes & Training teams, will ensure that all EO employees are informed of their privacy responsibilities by:

- Developing and implementing privacy orientation and annual refresher training for EOHQ staff[5].
- Developing and implementing privacy and security orientation training for field staff, along with static reference materials.
- Providing all new EOHQ employees and key staff with a copy of the EO privacy policies and procedures on their first day of employment (i.e. within the on-boarding package); and providing poll officials with a summary of key privacy considerations in the CEO's letter to poll officials.
- Communicating to EO personnel and service providers about privacy issues and risks throughout the year, as required.

5.12.2 Training must reflect key content from EO's privacy and security policies, including EO's privacy responsibilities, how to recognize PI, how to respond to a privacy breach, and safeguards for PI.

5.12.3 EO personnel should retake training annually, where applicable.

5.13 Monitoring and Enforcement

5.13.1 EO monitors organizational compliance with this policy under the direction and oversight of the CPO. Activities to monitor and gauge the efficacy of the privacy program will include:

- A review of privacy policies, procedures, and training at minimum once every general election cycle, led by Corporate Affairs.

[5] As of this writing, updated training is being developed for EOHQ.

- A privacy and security questionnaire conducted at minimum once every year, led by the CPO, which will assess perceptions of the program and privacy and security awareness.
- Spot checks of compliance with privacy and security policies, such as clean desk checks, at random intervals, led by ITDS and assisted by others within the Privacy Office.
- Audits of third-party premises and documentation on a regular basis and/or as the need arises, where agreements allow.
- Conducting more extensive privacy self-audits as appropriate.

5.13.2 To ensure that EO's initiatives reflect the 10 principles set out in this policy, and in accordance with privacy best practices, the relevant lines of business shall ensure that any privacy impact assessments (PIAs):

- Are initiated early in project development or design.
- Are completed prior to project implementation and that any risks are mitigated, transferred, avoided, or accepted (with a plan in place to resolve the risk), prior to migrating any components to production which would impact how EO collects, uses, retains, discloses, secures or disposes of PI.
- Are refreshed in response to project scope or implementation changes.

5.13.3 EO employees and agents in breach of this policy could be asked to retake their privacy and security training. They may also face disciplinary action, which may include termination of employment or contract or legal action.

5.13.4EO contractors and sub-contractors in breach of this policy will be subject to consequences set out in relevant agreements, which may include termination of the agreement relationship.

5.13.5 All EO agents, as well as political entities, are subject to the rules and consequences set out in the *Election Act* and *Election Finances Act*.

Section 6: Roles & Responsibilities

6.1 Chief Electoral Officer

The CEO is responsible for oversight and management of the privacy and security management programming. This includes:

a) Providing strategic direction on EO's privacy and security program, based on advice from the CPO, the IPC, and best practices of other electoral management bodies (EMBs).

b) Reviewing escalated inquiries and complaints from the CPO and providing feedback or decisions.

c) Reviewing the CPO's annual privacy report and accepting or rejecting recommendations based on a comprehensive understanding of projected costs, benefits, and risks.

d) Incorporating meaningful program developments into the CEO's Annual Report to the Legislative Assembly of Ontario, pursuant to Section 114.3(1) of the *Election Act*.

6.2 Assistant Chief Electoral Officer

The ACEO may act in place of the CEO if required.

a) If acting for the CEO, the ACEO is accountable for the same responsibilities assigned to the CEO. Despite the above, care should be taken to avoid a conflict of interest where the CPO is the ACEO (e.g. it is generally recommended that the CPO not also be the individual to decide on the purpose and means of data processing).

b) At the discretion of the CPO and CEO, the ACEO may have further involvement in activities related to the privacy program. The ACEO should understand the privacy governance framework and EO's privacy and security policies and procedures. They may be requested to provide feedback regarding specific privacy issues and concerns related to their cluster.

6.3 Chief Privacy Officer

The CEO has delegated responsibility for the oversight and management of EO's privacy operations to the CPO. In this role, the CPO is responsible for:

a) Acting as the central privacy contact for the organization and the primary contact for employees, via priv@elections.on.ca.

b) Articulating the vision and strategy for EO's privacy program; overseeing the implementation of responsive privacy programming; and developing any goals, benchmarks and/or metrics in conjunction with the Privacy Office.

c) Participating in the development of privacy impact assessments (PIA) or preliminary assessments or allocating resources to do so.

d) Managing privacy and security breaches, in accordance with EO's Privacy and Security Breach Management Protocol.

e) Centrally tracking privacy issues and risks to resolution and reviewing these at least quarterly.

f) Overseeing and approving internal and external communications regarding the privacy program, such as bulletins and memos.

g) Making recommendations to review and/or audit aspects of privacy operations.

h) Making recommendations to review and/or audit the activities of a contractor or sub-contractor, or to take other measures that are provided for under EO's agreement with the contractor in response to a failure to adhere to privacy terms, a privacy risk, or a privacy breach.

i) Working with the Director, ITDS, on information security issues of mutual interest.

j) Hosting quarterly roundtables with the Privacy Office, as well as ad-hoc meetings where required, to discuss privacy-related matters as they may arise throughout the year, and communicating with the ACEO about privacy issues and concerns related to their cluster.

k) Reporting to the CEO and Senior Leadership Team (SLT) on the outcomes of quarterly touchpoints with the Privacy Office, as well as annually with respect to updates and recommendations for EO's privacy programming.

6.4 Privacy Office

The Privacy Office is responsible for assisting the CPO with privacy program implementation. They include:

a) Executive Assistant to the CPO

- Supporting the CPO, and acting as backup for the Manager, Compliance Enforcement, with respect to privacy inquiries and complaints.

b) Manager, Compliance Enforcement

- Regularly monitoring priv@elections.on.ca for issues related to privacy inquiries, complaints, risks, and breaches; this should be no less than daily.
- Advising on privacy and security risks and facilitating breach management and documentation, in accordance with the Privacy and Security Breach Management Protocol.
- Redirecting inquiries and complaints intended for the CPO to the Executive Assistant to the CPO.

c) Manager, Corporate Affairs

The Manager, Corporate Affairs, is the Privacy Office lead with respect to privacy policies and procedures. They are responsible for:

- Updating EO's policies, including privacy and security policies, based on a predetermined schedule at least once every general election cycle.
- Advising on new service agreements and information sharing agreements from a policy perspective; ensures that Procurement & Logistics is aware of and has access to the latest versions of privacy and security policies and procedures.
- Advising on the interpretation of privacy policies and procedures, and the development of related training activities and artefacts.
- Coordinating a privacy and security questionnaire at minimum once every year and summarizing results and trends for the CPO, SLT, and the Executive Committee.
- Conducting research on emerging issues, legislative updates, privacy breaches, and enforcement decisions, and advising the CPO on trends and developments that may impact EO's privacy strategy and programming.

- Communicating privacy requirements to the Political Advisory Committee and party representatives.

d) Director, ITDS

The Director, ITDS, is the Privacy Office lead with respect to IT security and technical safeguards. They are responsible for:

- Advising on the interpretation of information security policies and procedures; facilitates development of related training activities and artefacts.
- Advises on appropriate safeguards to facilitate protection of PI, including when it is being accessed, used, disclosed, transferred, returned, destroyed, and/or de-identified.
- Advising on the costs and benefits of adopting new products, services, modifications and improvements to IT infrastructure, upgrades to IT solutions, training courses, and methodologies that can help EO meet its privacy objectives or reduce privacy risks.
- Facilitating EO's adherence to the IT Access Control and User Access Management Policy, the Personal Information Use and Retention Procedure, and the Computer and Technology Acceptable Use Policy, including through spot checks.
- Working with the CPO on privacy issues of mutual interest. This will include facilitating the successful conduct of PIAs by providing in-house SMEs and/or working with service providers to conduct a PIA, including providing service providers with the relevant supporting documentation, policies, procedures, and training; and granting interviews as needed.
- In conjunction with EO's service providers, overseeing security monitoring and logging for EO's information systems, during and outside of events; and bringing privacy and security risks to the attention of the CPO.

The following other individuals may also be engaged as members of the Privacy Office on specific questions and concerns related to:

e) **Coordination of training:** Manager, Human Resources for EOHQ staff; Manager, Election Processes & Training for field staff. Training encompasses the deployment, tracking, and evaluation of both in-person and online privacy and security training.

f) **Service agreements, physical safeguards:** Manager, Procurement & Logistics.

g) **Information sharing agreements:** Manager, PREO.

Other SMEs may also be engaged by the CPO and the Privacy Office on an ad-hoc basis. In addition, public inspection of candidate nomination papers and election finances documents are overseen by the Manager, Election Infrastructure, and the Director, Compliance, respectively.

All members of the group are responsible for attending quarterly roundtables with the CPO, or more frequent meetings if required.

6.5 EO Personnel and Service Providers

All employees, contractors and sub-contractors, and agents of EO are responsible for:

a) Understanding and adhering to EO's privacy and security policies and procedures; in particular, they must only collect, use, and disclose PI for purposes that are aligned with this policy.

b) Providing the CPO and the Privacy Office with information and resources to understand and mitigate privacy risks and breaches.

c) Redirecting privacy-related inquiries and complaints to priv@elections.on.ca in a timely manner.

d) Reviewing ad-hoc communications (e.g. all-staff emails, notices) related to the privacy program in a timely manner.

e) Participating in privacy-related programming such as training, external audits, self-audits, and/or investigations.

Furthermore, it is the responsibility of each business that manages a relationship with a service provider to:

f) Exercise their rights under the agreement, including auditing the third-party premises and documentation on a regular basis and/or as the need arises.

g) To adhere to their responsibilities under the agreement, including developing appropriate procedures and training to ensure that these responsibilities are observed.

All service providers are responsible for:

a) Adhering to the terms of their contracts or agreements with EO as they relate to privacy and security requirements, including breach reporting and management requirements.

b) Adhering to applicable privacy laws and regulations.

Section 7: Additional References

The following table identifies those Elections Ontario policies and procedures that expand upon the Elections Ontario Privacy Policy.

Document Name	Author(s)
1. Guidelines for the Use of Electoral Products	Elections Ontario
2. Personal Information Use and Retention Procedure	Elections Ontario
3. Computer and Technology Acceptable Use Policy	Elections Ontario
4. IT Access Control and User Access Management Policy	Elections Ontario
5. Privacy and Security Breach Management Protocol	Elections Ontario
6. Recordkeeping Policy	Elections Ontario
7. Records Retention Schedule	Elections Ontario
8. Permanent Register, Absentee Register & Electoral Products Privacy Policy	Elections Ontario
9. Ontario Register of Future Voters Privacy Policy	Elections Ontario

Section 8: Approval

The following table shows the authorization, amendment, and review dates for this policy.

Elections Ontario Privacy Policy	
Authorization	Chief Electoral Officer Date: January 6, 2021
Effective date	January 6, 2021
Date last amended	January 2011
Date of next review (Once per election cycle)	December 16, 2024
Contact officer	Deborah Danis, Chief Administrative Officer and Assistant Chief Electoral Officer, Elections Ontario

Appendix A: Police Requests for Information

- EO will not disclose PI without the consent of the individual unless the disclosure is required by law, including to comply with a subpoena or warrant issued, or an order made by a court, person or body with jurisdiction to compel the production of information; or to comply with rules of court relating to the production of records.
- All requests for information from PREO must be made in writing to the CEO, by email, fax, or regular mail. Requests must include the requesting officer's identity; the police service or government agency to whom the information will be provided; the active investigation under which the information is being sought; and whether the information is being requested under a court order, warrant or legislative provision authorizing collection of the information by the officer. It must also set out the specific information that is being sought. EO may request clarification for requests that are overly broad.
- EO will allow police to request information without a court order only if the matter involves a risk of immediate physical danger to an individual and if the disclosure will not intrude on a reasonable expectation of privacy[6].
- Release of PI to the police should only take place where it is legally required (by search warrant or production order) or to aid in a specific investigation, where the proposed disclosure would not infringe on the individual's reasonable expectation of privacy. Data minimization and necessity should guide the disclosure; in general, the minimum amount of information requested to facilitate the request should be disclosed.
- Notification of the individual after the fact is necessary if the disclosure took place for health or safety reasons. It should also be

[6] In determining whether a reasonable expectation of privacy exists, EO will consider guidance from the IPC related to other public sector organizations.
e.g., IPC. (2019). *Release of personal information to police: your privacy rights*. https://www.ipc.on.ca/wp-content/uploads/2019/08/fs-privacy-release-of-pi-to-police-your-privacy-rights.pdf

considered under other circumstances where it would not infringe on the investigation.

- EO will document the nature and extent of informal police requests as well as the circumstances under which records are disclosed.