Privacy Policy of the Ontario Party

Publication of the Policy

Once accepted by Elections Ontario, the Privacy Policy of the Ontario Party shall be published on the official Ontario Party website (ontarioparty.ca) within 30 days of receiving an acceptance confirmation from Elections Ontario.

Section 1: Scope of Policy

Whereas Section 17.6 of the *Election Act* requires political entities who wish to access electors' personal information held by Elections Ontario to develop and implement a privacy policy, the Ontario Party does hereby set forth the following Privacy Policy to govern the use and storage of any List Products from the Permanent and Absentee Registers provided by Elections Ontario.

This Privacy Policy shall apply to all staff, volunteers, representatives, agents, and associates of the Ontario Party and any vendors or suppliers put to use by the Ontario Party that will access the data received via the List Products.

Section 2: Restriction on Use

As per Section 17.4 of the Election Act, all data received by the Ontario Party from Elections Ontario via the List Products will be used for electoral purposes only and shall not be used for commercial purposes.

The Data shall be used by authorized individuals exclusively for the advancement of the political goals of the Ontario Party, in order to and by means of identifying and communicating with voters.

Distribution and access to The Data will be centrally tracked and controlled by the duly appointed Chief Privacy Officer of the Ontario Party by means of the completion of copies of Elections Ontario Forms F0101 and F0315 or their functional equivalents, whether in digital or hard copy forms.

All individuals that will be accessing The Data must first correctly complete a Form F0101 and return it to the Chief Privacy Officer. The submission of the completed form shall serve as the official request to receive authorization to access The Data. No access to the Data shall occur without submission of the F0101 Form and the prior authorization by the Chief Privacy Officer.

A correctly completed Form F0101 constitutes a written acknowledgment that the individual agrees to be bound by the restrictions set forth in Section 17.4 of the Election Act.

Section 3: Privacy Requirements

3.1 Implementation and Enforcement of Privacy Controls

Administrative controls

All access to The Data shall be granted on a strictly "need to know" basis, as determined by the Chief Privacy Officer or his or her duly appointed deputies for those purposes. Any individuals requesting access to The Data shall be assessed by the Chief Privacy Officer or his or her duly appointed deputies for fitness and ability to maintain responsible privacy safeguards while accessing The Data.

Technical controls

All digital storage and access of The Data shall conform to reasonable modern best practices for password requirements, audit trails, encryption, firewalls, and any other technical security safeguards to minimize the risk of unauthorized individuals accessing The Data.

These best practices shall be determined by an expert in the field of Information Technology and may be compiled into a guiding document, which may be subsequently used as reference and updated as needed at the request of the Chief Privacy Officer.

At a minimum, all digital access to The Data shall be protected by limiting access to password-protected user accounts. Any user accounts with remote access shall not be shared with any other individual, regardless of their authorization status.

Any hardware used to store The Data digitally shall be subject to the limitations set forth in the section detailing "Physical Controls" of the Privacy Policy.

Physical controls

All physical storage and access of The Data shall conform to reasonable modern best practices for document security to prevent unauthorized individuals from physically accessing The Data.

At a minimum, physical copies of The Data shall be stored in a location that can prevent physical access to unauthorized individuals, and only required physical copies limited to the scope of a political activity (for example, a canvassing sheet for a given geographical area) may be handled by an individual outside of the restricted area where The Data is stored. Any such copies shall be returned to a physically secure location for storage, or immediately destroyed, and may only be handled by individuals authorized to handle them.

3.2 Disposition Protocol for List Products

Any copies of The Data no longer required for electoral purposes and which cannot be securely stored, shall be disposed of in compliance with the Secure Destruction of List Products. Methods used for disposal, whether in digital or hard copy form, shall ensure that personal records contained in The Data cannot be reconstructed.

Data erasure must conform to the standard set by the Communication Security Establishment Canada wiping method.

Destruction of hard copies shall be by means of cross-cut shredding, and not single-strip (continuous) shredding.

3.3 Training on Privacy Controls

Any individuals accessing The Data or any selections extracted from it shall be trained in the proper handling of the data, and shall be required to read, understand and abide by the Privacy Policy of the Ontario Party. Such training shall be carried out by the Chief Privacy Officer or his or her duly appointed deputies.

3.4 Breach Management

Any accidental or unauthorized access, disclosure, use, modification, and disposal of The Data shall immediately be reported to the Chief Privacy Officer who shall evaluate the scope of the breach and inform the Chief Electoral Officer in the case of loss, theft of, or unauthorized access to, electors’ personal information.

Where a security flaw is identified, the Chief Privacy Officer shall determine the appropriate measures of mitigation, including removal of authorization to any compromised individuals, user accounts, or transferring of The Data to a more secure storage location or facility.

Section 4: Roles and Responsibilities

The Ontario Party's Chief Privacy Officer is the signatory on the Privacy Policy and is responsible for:

- ensuring the safeguarding of electors’ personal information against accidental or unauthorized access, disclosure, use, modification, and disposal;
- complying with all Elections Ontario filing requirements; and
- the overall implementation, updating, and enforcement of the privacy policy.

It is the personal responsibility of all individuals granted access to The Data to abide by the Privacy Policy, and report any breaches or suspicious activity relating to access or use of The Data to the Chief Privacy Officer.

Section 5: Privacy Policy Approval

The Privacy Policy of the Ontario Party is effective as of April 22, 2022.