

Elections Ontario Privacy Policy

New Blue Party of Ontario

Date of Creation: September 22nd, 2021

1.0 Scope of Policy

This privacy policy (the “Privacy Policy”) applies to the New Blue Party of Ontario and any person or entity representing or working for the Party on a paid or unpaid basis (the “Party”). The Privacy Policy applies to all list products received from Elections Ontario. The Privacy Policy ensures compliance with the restrictions on the use of the information extracted from the permanent register and absentee register under section 17.4(1) of the *Election Act* and requires that the information in list products received from Elections Ontario are securely maintained and confidentiality is protected.

2.0 Restrictions on Use

The Party acknowledges that the use of list products containing electors’ personal information is for electoral purposes only (communicating with voters, soliciting campaign support, recruiting party members, etc), and cannot be used for commercial purposes. The distribution of these lists to other authorized persons, can only occur once written acknowledgment from the recipient has been received. The written acknowledgment form that is provided in Appendix B of this Privacy Policy will be used.

Each individual will confirm in the written acknowledgement that he / she:

- a. understands that the list products can only be used for electoral purposes and not for commercial purposes;
- b. understands the importance of protecting electors’ personal information on the lists;
- c. undertakes precautionary measures to protect confidentiality of electors’ personal information (i.e. properly handling and transporting list products); and
- d. will return the lists on completion of the task for which the lists were provided to recipient.

3.0 Privacy Requirements

A distribution tracking record will be implemented and maintained as shown in Appendix C and Appendix D to this Privacy Policy to monitor who has been given access to electors’ personal information, whether in portions or in entirety.

This tracking system will capture:

- a. the date of distribution;
- b. the format in which the document was distributed (i.e. electronic or paper copy);
- c. the name of the individual that this information was provided to;
- d. the type of list products (e.g. annual update, preliminary list of electors, or advance poll list of electors’, etc);
- e. confirmation that the written acknowledgement has been signed; and
- f. confirmation of the date the copy was returned to the Political Entity or a certificate of destruction

The Party acknowledges that any part of the information obtained electronically from the permanent register, including the list of electors, may not be reproduced, stored, or transmitted, except as follows:

- a. the Party receives an update of the permanent register for the whole of Ontario as a result of the annual update (section 17.1(3)(1)(i) or (ii) or have received an update with respect to a specific electoral district under section 17.1 (3)(2)); and
- b. an individual or entity who has received the information from the registered the Party, so long as that person or entity signs a written acknowledgement that they are bound by the restrictions in the *Election Act* on use of the information for electoral purposes only and not for commercial purposes (s. 17.4(4)(b)).

As part of efforts to protect electors' information in a mobile environment, employees, volunteers, and/or agents of the Party will follow the below Best Practices:

- a. List products will only be removed from the office when it is absolutely necessary to do so;
- b. Employees, volunteers or agents of the Party must obtain any approvals required, and where possible, original documents should remain in the office and only copies removed;
- c. A record of the information being removed will be kept in a safe location;
- d. While in transit, paper records will be securely packaged and locked and will remain in the possession of the employees, volunteers, or agents of the Party;
- e. If being used at home, records must be accessible only to the employees, volunteers or agents of the Party and will be kept locked away when not in use;
- f. While traveling on public transit, electors' personal information will never be accessed either digitally or printed, by volunteers, employees, or agents of the Party;
- g. Electronic records containing electors' personal information will be stored and encrypted on password protected data storage devices and apps, or removable drives rather than on the hard drive of a laptop or home computer;
- h. Removable drives will always remain within the possession of the employees, volunteers or agents of the Party or be kept in a secure location that is not accessible to others;
- i. Access to laptop, home computers, will be password-controlled, and any data on the hard drive must be encrypted. Other reasonable safeguards, such as anti-virus software and personal firewalls, could also be installed;
- j. List products containing electors' personal information will not be stored on shared computers and laptops;
- k. Laptops will always be stored in a secure location;
- l. Access to wireless devices such as cell phones, that have personal information stored on them, will be password-controlled and the data stored will be data encrypted;
- m. While working at locations outside the office, employees, volunteers, or agents of the Party will maintain constant control of wireless devices and care will be taken to prevent loss or theft;
- n. While working from home or at other locations outside the office, employees will avoid sending electors' personal information by email or fax; and
- o. When photocopies of list products are required, employees of the Party must conduct the task and photocopy machines must not be left unattended

Should a suspected or actual privacy breach occur, it will be dealt with quickly and effectively by the Chief Privacy Officer (please see “Roles and Responsibilities” below for general steps.)

All products will be destroyed as per Section 6 of Election Ontario Guidelines for the Use of Electoral Products and the Party shall use Appendix E included herein. A certificate of destruction will be filed with the Chief Electoral Officer or the Returning Officer as appropriate, by November 30th of the calendar year for the Annual Release, and within 30 days after polling day for the Lists of Electors for Electoral Events.

4.0 Roles and Responsibilities

In order to prevent unauthorized parties from accessing electoral information, including taking steps to protect electoral information during storage, transportation, handling and destruction, a person will be appointed to be responsible for safeguarding electoral products. This person would be responsible for communicating these Guidelines to persons who are given access to electors’ personal information, for developing and implementing privacy policies and answering questions about the Party’s use of list products. This person must hold the title of Chief Privacy Officer. Elections Ontario will be notified once the person no longer holds the title and an updated privacy policy will be submitted.

The Chief Privacy Officer shall:

- a. provide clear direction to his/her candidate, members, employees, and agents regarding the proper use of the information obtained from the permanent register, absentee register and other electoral products;
- b. provide electoral products only to individuals who need access to electoral products to communicate with electors and constituents on behalf of Party or to do work for electoral purposes on behalf of the Party;
- c. limit the number of people who have access to reduce the chances of a privacy breach;
- d. ensure that the electoral products are kept secure when not in use by storing the electronic copy on a secure, password-protected computer and keeping paper copies in locked filing cabinets;
- e. strictly control all passwords and keys;
- f. ensure that all individuals who are given access to electors’ personal information understand the importance of protecting the privacy of electors’ information; and
- g. obtain from each individual a written acknowledgement that the individual will abide by the restrictions on the use of electors’ personal information.

In the event of a privacy breach, the Chief Privacy Officer will follow these general steps, understanding that each situation will be unique and will need a customized approach:

- a. notify Elections Ontario of the breach and steps being taken to contain/mitigate the breach;
- b. contain the breach and identify the source;
- c. mitigate the harm resulting from the breach;
- d. retrieve any documents that were lost or stolen;
- e. document the circumstances that led to the incident and/or contact the police; and
- f. review and update the internal policies, processes, and procedures to prevent a future incident.

5.0 Training and Compliance

To ensure awareness and compliance, training (on an annual basis) on this privacy policy and its controls and regulations, will be part of the onboarding process for high-level volunteers or staff of the Party, who receive, have access to, or work with, PREO products received from Elections Ontario.

6.0 Approval

This privacy policy is effective as of the date of approval by Elections Ontario.

 _____ (Signed)

Date: September 22, 2021

Allison Bruns
Chief Administrative Office and Chief Privacy Officer
New Blue Party of Ontario