

Privacy Protection Policy

Policy Statement

Elections Nova Scotia (ENS) respects the privacy of electors in Nova Scotia and is committed to protecting the integrity of electoral information. ENS has developed this policy regarding privacy protection to ensure that elector personal information collected by the agency is appropriately protected, used for electoral purposes only, and the privacy and security of the data is maintained.

This policy is the foundation of Elections Nova Scotia’s privacy protection framework, which includes guidelines for registered political parties and candidates to encourage them to implement privacy measures to protect elector personal information released to them by ENS.

Authority

Elections Act (the Act)

The *Act* provides for disclosure of preliminary, revised, official and final list of electors. The *Act* authorizes disclosure to different bodies at different times. The elector personal information provided by ENS to registered parties and candidates must only be used for electoral purposes.

The below chart summarizes what information, to whom, and at what time extracts of the register of electors and the list of electors may be provided:

List	Authorized Disclosure	Timing	Section
Extract of Elector Information from the Register of Electors (legal name, residential address, mailing address, elector’s unique identification number on the register, age range category) and an indication whether the elector voted in previous elections commencing with the general election held on June 9, 2009	Registered Party	At time determined by Chief Electoral Officer (CEO)	44(1) (a)
Same as above but only for the electors in the member’s electoral district	Independent Member of the House of Assembly		44(1)(b)

Preliminary List of Electors – Information of electors in the Candidate’s electoral district extracted from the provincial List of Electors used for the election event (legal name, residential address, mailing address, elector unique identification number, age range category, an indication whether the elector voted in previous elections, and whether the elector voted in the current election as of time of disclosure)	Nominated Candidate	As soon as possible after the writ of election is issued	52(3)
Revised List of Electors. As above but does not include the indication whether the elector voted in previous elections.	Nominated Candidate	Before an advance poll	57(1)
Official List of Electors – similar to the Revised List of Electors	Nominated Candidate	After the close of advance polls and Before election day	57(3)
Final List of Electors – Elector information for all electoral district in which the party nominated candidates (legal name, residential address, mailing address)	Registered Party	Within 60 days after election day	59(4)
Final List of Electors	Independent elected Member of the House of Assembly		59(4)

Freedom of Information and Protection of Privacy Act (FOIPOP)

In Nova Scotia, *FOIPOP* details the laws concerning the privacy of individuals with respect to personal information held by public bodies. *FOIPOP* applies to all records in the custody or under the control of a public body and provides parameters for the collection, protection, retention, use and disclosure of personal information. ENS is a public body under *FOIPOP*, and thus must comply with *FOIPOP* except where the *Elections Act* expressly exempts its application such as in subsection 62(3).

Under *FOIPOP*, a public body may not collect personal information unless expressly authorized to do so. Similarly, a public body may only disclose personal information as provided pursuant to another enactment, and the disclosure must be made in accordance with *FOIPOP*.

The Chief Electoral Officer (CEO) is required to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or disposal of information. Thus, to comply with *FOIPOP*, ENS must be satisfied any personal information provided to candidates or registered political parties will be stored securely and only used for electoral purposes.

Registered political parties in Nova Scotia are not considered “public bodies” and are not subject to *FOIPOP*.

Definitions

TERM	DEFINITION
Elector Personal Information	Any personal data such as an elector's name, address, and birth date, that is collected for electoral purposes by ENS. The List of Electors and Nova Scotia Registry of Electors as defined below are examples of elector personal information maintained by ENS.
Electoral Purposes	Means for administering elections or by-elections including communicating with electors during an electoral event and for soliciting contributions and campaign support.
List of Electors	An extract from the Nova Scotia Registry of Electors, which consists of elector and address data. It is prepared by the Chief Electoral Officer (CEO) following the writ being issued for use at a general election or a by-election. For purposes of these privacy protection guidelines the List of Electors is considered elector personal information.
Nominated Candidate	A person who has been officially nominated as a candidate at an election endorsed by a registered party or declared as an independent candidate pursuant to Section 67 of the <i>Act</i> . Candidates' nomination documents must be approved by the RO before they receive the List of Electors for their electoral district.
Nova Scotia Register of Electors	An up-to-date database of eligible Nova Scotian voters who registered to vote in the province. The Register contains the elector's name, address, and birth date. It is maintained for electoral purposes only. For purposes of these privacy protection guidelines the Nova Scotia Register of Electors is considered elector personal information.
Political entities	For the purpose of this policy political entities are considered registered political parties in Nova Scotia, candidates (independent or part of a political party) and independent candidates or MLAs.
Privacy Breach	Loss, theft, unauthorized access or misuse of elector personal information constitutes a privacy breach and should be dealt with quickly and effectively. If a copy of the List of Electors is lost or stolen, elector personal information could be used for unauthorized purposes and is considered a privacy breach.
Privacy Protection Policy	Governs how the agency handles personal information it collects. Outlines the reasonable precautions to ensure the security of personal information.

Secure Storage	The manual and automated computing processes and technologies used to ensure stored data security and integrity. This can include physical protection of the hardware on which the data is stored.
----------------	--

Policy Overview

ENS has developed this privacy protection policy to govern how the agency handles the elector personal information it collects and shares with registered political parties and candidates. The policy outlines how the agency takes reasonable precautions to ensure the privacy and security of elector personal information. The policy also outlines the processes in place to track the distribution of elector personal information, and the procedures that would be engaged in the case of a privacy breach.

This policy is the center of ENS’s privacy protection framework, which includes the Privacy Protection Guidelines for Registered Political Parties and Candidates.

Scope

This policy applies to all elector personal information collected and stored by ENS. The purpose of the policy is to ensure that elector personal information is appropriately protected, used for electoral purposes only, and the privacy and security of the data is maintained.

Accountability and Responsibilities

ENS is responsible for the security and integrity of elector personal information and shall safeguard such information against accidental or unauthorized access, disclosure, use, modification, and disposal.

Policy Directive

Security

For purposes of this policy, the following measures are considered reasonable precautions:

- All ENS staff and election workers with access to, or a copy of, elector personal information must take reasonable precautions to protect the security and confidentiality of the information and must sign a confidentiality agreement to this effect.
- All election workers with access to, or a copy of, elector personal information must take an oath to protect the security and confidentiality of that information
- Registered parties, independent MLAs, and candidate are required to:
 - o Provide clear direction to all authorized recipients regarding the proper use of elector’s personal information obtained from the Register of Electors and electoral products.

- Provide staff training to educate on privacy methods and the importance of protecting elector personal information.
- Provide electoral products only to people who need access to communicate with electors and constituents on behalf of the political entity or to do work for electoral purposes on behalf of the political entity.
- Designate a person who will be responsible for implementing privacy safeguards.

Technical measures:

- Ensure that the electoral products are kept secure when not in use by storing the electronic copy on a secure, password-protected computer.
- Ensure that the digital electoral products are stored in encrypted formats on any used computers and servers and storage units such as USBs.
- Passwords for computers and encrypted information and USB keys should be strictly controlled by the person responsible for privacy safeguards.
- Encryption, firewalls, and other technical security safeguards should be used to minimize the risk of unauthorized individuals accessing personal information.

Physical measures:

- Restrict access to areas where personal information is stored.
- Keep paper copies in locked filing cabinets. It is also preferable to avoid paper copies of the information, where possible.

Tracking and Distribution


If ENS provides any other individual or entity with access to, or a copy of, personal information, the following information must be tracked and retained:

- The date of provision of access, or distribution.
- To whom the personal information was provided to.
- What personal information was provided.
- How the personal information was provided (e.g. access to database, provision of electronic copy of record, provision of paper copy of record, etc.).
- Confirmation that the individual or entity has read this policy and agrees to be bound by it.
- Confirmation of the date the personal information is returned or destroyed.

Breach Procedures

In the case of loss or theft of, or unauthorized access to personal information, the following procedures must be followed:

- The breach should be contained, and the source of the breach identified.
- The loss, theft or unauthorized access must be reported to the CEO.
- Affected individuals must also be notified if there is a risk.
- The loss, theft or unauthorized access must be reported to the Information Access and Privacy (IAP) Services Division.
- All personal information lost must be retrieved, if possible.
- The circumstances that led to the incident must be documented.
- Internal policies, processes and procedures must be reviewed to prevent future incidents.

CR File No:		
Prepared by: Naomi Shelton, Director of Policy and Communications Date: September 14, 2022		Effective Date: October 1, 2022
Approved by: Lindsay Rodenkirchen, Acting Chief Electoral Officer Signature:  Date: September 14, 2022		Reviewed by: Date:
Version No.: 1.0	Change Date:	Change Description:
Review Frequency: Every two years - first review due October 1, 2024		