Effective: January 1, 2024

Privacy Protection Guidelines for Political Entities

Background

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

ENS policy has informed these Privacy Protection Guidelines for Political Entities in Nova Scotia. For the ENS policy and these Guidelines, registered political parties, candidates, and independent MLAs are jointly referred to as "political entities". The Guidelines include a privacy best practice summary, a Declaration Form, a Certificate of Destruction Form and protocols for safe disposal and reporting privacy breaches.

ENS requires all political entities to read the following guidelines and submit a signed Declaration Form (Appendix A) to attest to their understanding of the privacy requirements for access and use of elector personal information. This process is in place to ensure that political entities have privacy practices that will help protect elector personal information released to them by ENS.

Policy Alignment

Elections Nova Scotia Privacy Protection Policy

The ENS Privacy Protection Policy outlines the procedures ENS takes internally to protect elector personal information in Nova Scotia. The ENS Privacy Protection Policy is the basis of its privacy protection framework, which includes these Privacy Protection Guidelines for Political Entities.

Definitions

TERM	DEFINITION
Best Practice	A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption.
Elector Personal	Any personal data such as an elector's name, address, and birth date, that is collected for electoral purposes by ENS. The List of

Information	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 preparing for and engaging in communications with electors, fund raising and campaigning during, and between electoral events.
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 *Act*. 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 document this refers to 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.

Overview

To assist political entities in meeting the privacy requirements laid out in the *Elections Act*, ENS provides these privacy protection guidelines and requires a signed declaration. These guidelines are a key part of ENS's privacy protection framework based on the ENS Privacy Protection Policy. The purpose of ENS's privacy protection framework is to improve the protection of the elector personal information.

ENS's privacy protection framework is rooted in best practice understanding gained from a jurisdictional scan of other provincial election management bodies, and an academic review of privacy protection articles. These best practices are documented in Appendix B and can be used to guide the practices of a political entity.

Accountability and Responsibilities

Elections Nova Scotia

- ENS is responsible under *FOIPOP* and the *Elections Act* for the privacy and security of elector personal information collected for electoral purposes.
- ENS is responsible for the secure release of extracts of the Register of Electors to registered political parties and the List of Electors to nominated candidates of their electoral district under the *Act*. Nominated candidates are not required to receive the LOE.
- ENS may use fictitious information about persons who reside in the province for the purpose of tracking the distribution of elector personal information and detecting privacy breaches when they occur.
- ENS is responsible for the development and maintenance of their privacy protection framework, which includes the ENS Privacy Protection Policy, these Guidelines, disposal protocols and breach protocols.
- ENS will maintain a register of all lists distributed by date, and the date of return for an attestation of destruction.

Political Entities

- Political entities are responsible to comply with the *Act*.
- Political entities are responsible to read and understand the ENS Privacy Protection Guidelines for Political Entities and to submit a signed declaration of acknowledgement indicating their responsibility for all who receive access to elector personal information during an electoral event within their organization
- Political entities are accountable for the responsible use by their staff and volunteers of the elector personal information released to them by ENS, and to ensure the use of the information is for electoral purposes only.
- Political entities are accountable for the privacy and security of the elector's personal information released to them by ENS.
- Political entities are required to securely dispose or recover and return to ENS all the elector personal information released to them when no longer required for the purpose for which it was released. Documentation of destruction is required (See

Appendix D for template). As per the *Act*, during an electoral event this must be done within thirty days after the closing of polls on election day.

GUIDELINES

Details of Elector Personal Information

The *Election Act* (Sec. 42(1)) requires that the Chief Electoral Officer establishes and maintains a Register of Electors for the Province that includes up-to-date information for each elector.

Under Sec. 44(1)(a) & 44(2), the CEO shall disclose this information to the political entities in the form of the Register of Electors, or an extract of the Register, known as the List of Electors. This information is to be used only for electoral purposes and includes the following elector information:

i. Residential address
ii. Mailing address
iii. Legal name
iv. Age range category
v. The assigned unique identification number on the register of electors
vi. An indication whether the elector voted in previous elections commencing with the general election held on June 9, 2009

Authorized Use of Elector Personal Information

The *Election Act* provides specific restrictions with regards to the appropriate use of elector personal information and all authorized recipients must adhere to the restrictions. It is an offence under the *Election Act* (Section 333) to use elector personal information for any purpose other than electoral purposes. For the protection of privacy, the ENS guidelines define electoral purposes as follows:

1. Communicating with electors during an electoral event
2. Soliciting of political contributions
3. Campaigning

Elector personal information shall not be used for any purpose that is not contained in the above-mentioned section, including but not limited to:

- Commercial use
- Selling of information
- Personal use

The obligation to comply with the authorized use of elector personal information applies to any person or entity who receives and examines the information in printed or electronic format or on data storage services and applications.

Requirements for access and use

ENS requires political entities to ensure their employees and volunteers comply with the restrictions on the use of elector personal information. By signing the declaration form (Appendix A), political entities are indicating they accept responsibility for the use of elector personal information by their employees and volunteers. Employees and volunteers do not need to sign the declaration form but have the same responsibility to follow these privacy protection guidelines.

Privacy measures

All individuals with access to elector personal information must take reasonable precautions to protect the security and confidentiality of the personal information.

For purposes of these ENS Privacy Protection Guidelines, the following provides direction on what measures are considered reasonable precautions:

Administrative measures:

- For purposes of this measure, "staff" refers to paid employees of the Political Entities and not volunteers
- Provide clear direction to all authorized recipients regarding the proper use of elector personal information
- Staff training on privacy to educate on privacy methods and the importance of protecting personal information
- Provide elector personal information 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
- Designating a person who will be responsible for implementing privacy safeguards

Technical measures:

- Ensure that elector personal information is kept secure when not in use by storing the electronic copy on a secure, password-protected computer
- Ensure that the digital copies of elector personal information are stored in encrypted formats on any used computers and servers and storage units
- Passwords for computers, encrypted information, and 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 elector's personal information

Physical measures:

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

Breach procedures

If a physical or digital copy of elector personal information is lost, stolen, or accessed without authorization, it could be used for unauthorized purposes. Loss, theft, unauthorized access, or misuse of information therefore constitutes a privacy breach and should be dealt with quickly and effectively. While each incident will require a unique approach, it is recommended that the person responsible for privacy safeguards follow these general steps:

- Contain the breach and identify its source;
- Document the circumstances that led to the incident;
- Review internal policies, processes, and procedures to prevent future incidents; and
- Report the breach to the CEO within 48 hours from when the breach occurred.

ENS's breach procedures are rooted in best practice understanding gained from internal policy and Nova Scotia's Information Access and Privacy (IAP) Services. These best practices are documented in Appendix B and can be used to guide the practices of political entities.

Disposal procedures:

Under Section 62(2) of the Elections Act, all political entities must dispose of elector personal information in a safe and secure way within thirty days of the close of the polls on election day. Reasonable steps must be taken to protect the security and confidentiality of elector personal information that is to be destroyed, including protecting its security and confidentiality during its storage, transportation, handling, and destruction. To prevent unauthorized parties from accessing elector personal information, it is important to use care in the disposal and destruction. The following provides guidelines for political entities on how to dispose of elector personal information in a safe and secure manner:

1. Methods used must ensure that personal records cannot be reconstructed.

2. For printed copies, destruction means cross-cut shredding, not simply continuous (single strip) shredding, which can be reconstructed.

3. For electronic and wireless media, destruction means either physically damaging the items (rendering them unusable and discarding them and employing wiping utilities provided by various software companies to erase every bit of data on a drive).

Enforcement:

Under Section 314B of the *Elections Act*,

A candidate or registered party that fails to destroy the list of electors and report the destruction as required by subsection 62(2) within thirty days of the close of polls on election day may be subject to a penalty of fifty dollars for each day that the candidate or registered party fails to destroy the list and report the destruction to a maximum of one thousand five hundred dollars.

Documentation:

Political entities should create a certificate of destruction that documents the following information:

- description of the records that are being destroyed;
- the date, time and location of destruction;
- the method of destruction; and
- the name and signature of the individual responsible for destruction.

A template for the Certificate of Destruction can be found in ***Appendix D.***

If the political entity has an external company that provides secure destruction services, a Certificate of Destruction must be provided by the shredding company. All Certificates of Destruction must be submitted to ENS at *elections@novascotia.ca.*

Guiding Principles

The privacy protection guidelines developed by ENS are a guide for political entities. All political entities must read and understand the ENS Privacy Protection Guidelines for Political Entities.

ENS will not provide extracts of or lists of the registered elector information to a political entity without first receiving a signed Declaration of Acknowledgement. (Form is in Appendix A).

APPENDIX A – Declaration of Acknowledgement for Use of Elector Information

FOR USE BY **REGISTERED PARTIES** (see next page for candidate/MLA template)

Please complete and sign the declaration page below and email a scanned copy to ENS at elections@novascotia.ca

In accordance with the *Elections Act*, I acknowledge the following regarding the information I obtain, directly or indirectly, related to elector personal information released by ENS during an election event, whether the information obtained is in printed or electronic format or examined in either format without obtaining a copy:

I, _____, duly authorized representative of the

_____ (name of registered party), hereby declare on behalf of the party, and not in my personal capacity, to adhere to the following conditions of release on the <*ADD DATE*> _____ :

1. To read and understand the ENS Privacy Protection Guidelines for Political Entities, including the best practices document;
2. To maintain the privacy and security of the elector personal information during the entity's use of the information by following privacy protection best practices;
3. To use the elector personal information received for electoral purposes only as defined in the ENS Privacy Protection Guidelines for Political Entities;
4. To adhere to the destruction requirements set out in the Guidelines and to provide a Certificate of Destruction as required;
5. To follow the privacy breach protocol in the event of a privacy breach; and
6. To inform all persons who are provided access to the elector personal information of the responsibilities in paragraphs 2,3,4 and 5 in such manner as is applicable to their level of access and permitted use.

_____, (Signature)

_____, (Position)

DATED at _____, on _____, 20__.

Declaration of Acknowledgement for Use of Elector Information

FOR USE BY **CANDIDATES AND INDEPENDENT MLAs**

Please complete and sign the declaration page below and email a scanned copy to ENS at elections@novascotia.ca

In accordance with the *Elections Act*, I acknowledge the following regarding the information I obtain, directly or indirectly, related to elector personal information released by ENS during an election event, whether the information obtained is in printed or electronic format or examined in either format without obtaining a copy:

I, _____, nominated candidate for the electoral district of _____ <name of the electoral district>, hereby declare to adhere to the following conditions of release of the List of Electors for my electoral district:

1. To read and understand the ENS Privacy Protection Guidelines for Political Entities, including the best practices document
2. To maintain the privacy and security of the elector personal information during the entity's use of the information by following privacy protection best practices;
3. To use the elector privacy information received for electoral purposes only as defined in the ENS Privacy Protection Guidelines for Political Entities;
4. To adhere to the destruction requirements set out in the Guidelines and to provide a Certificate of Destruction as required;
5. To follow the privacy breach protocol in the event of a privacy breach; and
6. To inform all persons who are provided access to the elector personal information of the responsibilities in paragraphs 2,3,4 and 5 in such manner as is applicable to their level of access and permitted use.

_____, (Name)

_____, (Signature)

DATED at _____, on _____, 20__.

APPENDIX B – PRIVACY PROTECTION BEST PRACTICES

Privacy policies

Regardless of whether a public entity has its own privacy policy, individuals have the right to complain and redress about their privacy policies[1]. Privacy management can increase civic trust, which is beneficial for public entities[1].

Privacy policy in the electoral process is no different than any other public realm. Electors have a reasonable expectation for the privacy of any personal information collected for electoral purposes. Election management bodies and political entities have a responsibility to protect the privacy of elector personal information.

A strong privacy policy establishes a clear governance framework and helps to set out roles and responsibilities of various stakeholders[2]. Making it available internally online helps staff remain informed, while making it available publicly increases accountability.

Further, improving privacy policies can help promote Nova Scotia as a jurisdiction with strong privacy and security standards[2].

Secure Storage

Includes both digital and physical storage. Digital measures include ensuring data is stored on secure, password-protected computers. Access and passwords should be tightly controlled. Encryption, firewalls, and double-authentication measures are also recommended.

Physical storage requires that materials are kept in locked areas where access to area is tightly controlled.

Risk assessments should be conducted before storing personal data in digital and/or physical locations, and ongoing assessment and practice of measures should be part of policies[3].

Training and education

Studies indicate that simply asking staff members to read and acknowledge their understanding of privacy policies is not enough[2]. Regular, and interactive training is necessary to create a workplace culture that prioritizes privacy measures.

Employing people who are appropriately skilled with the necessary skills and knowledge in personal data protection ensures expertise exists in the organization.

Data breach handling

An online internal platform for incident reporting allows for standardized and efficient reporting[2]. Recommended practices include: gathering essential information related to the breach, consider notifying regulatory bodies, decide on measures to contain breach, assess

the risk of harm, consider notifying the data subjects affected by the breach, investigate the data breach and report investigation results, and conduct post incident review[4].

Communication

It is helpful to nominate staff of different levels as data protection leads, who ensure data protection policies are being followed and reviewed appropriately[2]. Leads should engage in quarterly meetings to address privacy concerns and manage controls of operations. Departments can also create working groups that share learnings and best practices.

Ongoing assessment and revision

Establishing a regular audit and review process of privacy policies and program controls is recommended to ensure they are up to date with current needs. Formulate a compliance check mechanism for routine protection of voter database throughout all activities[3].

The following questions can help guide ongoing assessment of practices[5]:

- Who is using data in campaigns?
- What are the sources of campaign data?
- How does data inform communication?

Risks and challenges

Lack of financial resources, and/or capacities, such as expertise[2].

It can be a challenge to make those who do not handle data directly more aware of privacy policy importance.

Difficult to find a common approach in handling personal data if offices have different needs/practices[2].

Identifying these challenges within the organization will help ensure policies can address them.

The references below provided significant knowledge for the above best practices. These sources include further information and recommendations, including template forms for policies and assessments, that could be of use to political entities who wish to develop or reassess their practices.

References:

[1] Bennett, Colin. Data Driven Elections and Political Parties in Canada: Privacy Implications, Privacy Policies and Privacy Obligations (April 12, 2018). Canadian Journal of Law and Information Technology, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3146964

[2] Privacy Commissioner for Personal Data: 2018 Study Report on Implementation of Privacy Management Programme by Data Users (2018). Hong Kong. Available at sweep2018_e.pdf (pcpd.org.hk)

[3] Privacy Commissioner for Personal Data: Guidance on Election Activities (June 2020). Hong Kong. Available at 210x210mm EN_062020_01 (pcpd.org.hk)

[4] Privacy Commissioner for Personal Data: Privacy Management Programme (PMP) Manual (February 2014). Hong Kong. Available at grg_private_sector.pdf (pcpd.org.hk)

[5] Dommett, Katharine. Data-driven Political Campaigns in Practice: Understanding and Regulating Diverse Data-Driven Campaigns (December 31, 2019). Internet Policy Review: Journal on Internet Regulation. Volume 8, Issue 4. Available at policyreview-2019-4-1432.pdf

APPENDIX C – PRIVACY BREACH PROTOCOL

Privacy Breach Protocol

If a privacy breach does occur, it is important to take steps to address the issue. This process is called a privacy breach protocol. The steps outlined below provide political entities with directions to help guide you and your team through the privacy breach reporting process.

1. Identify the privacy beach

If the potential of a privacy breach has been identified, it is important to establish the date, time, type, and extent of the breach. Actions taken and decisions made during the implementation of the Privacy Breach Protocol should be documented, including the timelines and the person responsible for carrying out the action or decision.

2. Immediate remedial action

Identify what action needs to be taken to contain/stop the breach. You and your campaign team could consider the following:

- Are any of your copies of the list or register of electors missing, and if so, what steps could be taken to account for all the lists?
- Were all the copies destroyed as you attested to, and if not, what steps must be taken to secure and destroy any remaining copies?
- Were any copies of the list or register of electors shared inadvertently, and if so, what steps can be taken to contact the recipient(s) in an effort to contain the breach?
- Will the breach allow any unauthorized access to the list or register of electors, and if so, what steps can be taken to reasonably avoid any additional breach?
- If you determine that any electronic device or paper records containing the list or register of electors has been stolen, have you contacted ENS and the appropriate law enforcement authorities?

3. Internal notification

In the case of a privacy breach, it is important that you inform your campaign team so they can assist with the investigation.

4. Investigation and documentation

It is important to determine the extent/scope of the privacy breach and who is involved. When investigating a breach, you should document evidence about the incident to determine the series of events that led to the breach.

5. External notification

If you or your campaign team determine that the privacy of the list of electors has been breached, it is necessary to inform key stakeholders. You should report the breach to the Returning Officer in your electoral district and ENS as soon as possible, unless there is risk of interfering with a police investigation. Notification must occur within 48 hours of determining there has been a breach. After reporting the privacy breach to ENS, you and your campaign must consider whether one or more of the following needs to be notified:

- Individual(s) whose privacy has been breached on the list of electors;
- Law enforcement authorities; and/or
- The general public or media outlets.

6. Follow-up and long-term remedial action

Based on the nature of the privacy breach you and your campaign team will need to determine what steps are necessary for follow-up and remedial action. These actions should also have longer-term considerations, involving strategies to prevent the privacy breach from occurring again. The steps you choose to take could impact your reputation if the issue becomes public. You may need to seek legal counsel to advise you on the action to take.

APPENDIX D – CERTIFICATE OF DESTRUCTION

To be filled out and submitted upon destruction of Register and/or List of Registered Electors. Political entities must email it to: elections@novascotia.ca

Electoral District:	Candidate Name and Party, if applicable:
Date that the Register and/or List of Electors was issued:	
Name of individual or company who securely destroyed electronic or paper copies:	
Date of secure destruction	
Time of secure destruction	
Location of secure destruction	
Types of documents securely destroyed (Official List of Electors, Strike-off Information, etc.)	Paper type: How many copies were destroyed: Electronic type: How many copies were destroyed:
Method of secure destruction	Paper: Electronic:
Signature of individual or company representative who destroyed electronic files or paper copies	
If applicable, Certificate of Destruction provided by shredding company (attach copy of certificate if applicable)	Yes or No

Date:

Candidate signature: