Elections Prince Edward Island
A Non-partisan Office of the Legislature

GUIDELINES FOR THE USE OF ELECTORAL PRODUCTS FOR INDEPENDENT CANDIDATES

(LIST OF ELECTORS)

Definitions

Breach - means Breach of Information including but not limited to loss or theft, unauthorized use of information or use of information by unauthorized persons.

List - any reference to "List" means Voters List, or part of a Voters List

Political Entity – Means any Registered Political Party and Registered Candidate, including Independent Candidates.

Shared – Means access to, disclosure or use of

Section 1: Introduction

The *Election Act* requires the Chief Electoral Officer (CEO) to establish and maintain a permanent register of electors.

The purpose of these Guidelines is to provide authorized recipients (Political Entities) with the requirements in the *Election Act* and the privacy best practices for the use and access of the information contained in the permanent register. The Guidelines have been created to ensure the effective protection and management of the electors' personal information contained in the permanent register.

These Guidelines also include the privacy requirements pertaining to the distribution and use of derivative products and electoral products. Derivative products (also known as list of electors) are created from the permanent register at the beginning of an electoral event and maintained during the event under the authority of the Chief Electoral Officer. Electoral products refers to all election-related information distributed to authorized recipients during an electoral event. This includes electoral districts, polling divisions, polls and strike-off information.

The permanent register contains personal information including names, civic and mailing addresses, date of birth and unique identifier for each registered elector. Where applicable, the list of electors contains the names, unique identifiers and civic address including associated district and poll for each elector.

Elections PEI places high importance on ensuring the protection of personal information. It is therefore imperative for authorized recipients of electors' personal information to take appropriate measures, as described in these guidelines, to maintain the integrity of the administration of Prince Edward Island's electoral system.

Section 2: Distribution of Lists of Electors

The *Election Act* (Sections 62(2) and 65(5)(6)) require the distribution of electors' personal information to authorized recipients. Where, under the *Election Act*, the CEO is required to provide copies of lists of electors, extracts of or updates to the permanent register, or any other personal information of electors to a candidate or registered party, they will not provide any information about electors other than the following,

1. Name and unique identifier
2. Civic address and associated District and Polling division
3. Strike-off Information

Section 3: Authorized use of List of Electors

The *Election Act* provides specific restrictions with regards to the appropriate use of the list of electors or part of the list of electors. All authorized recipients must adhere to the restrictions to use the list of electors for electoral purposes only. It is an offence under the *Election Act* (Section 129.1(a)) to use information from the permanent register, or list of electors for any purpose other than the following;

1. Communicating with electors
2. Soliciting of contributions
3. Campaigning

> **129.1 Offences, use of list of electors**
> *"Every one is guilty of an offence who uses all or part of a list of electors for any purpose unless the list or part of the list is used*
> *(a) by a registered party, a member of such a party or a member of the Legislative Assembly for the purpose of communicating with the electors, including the soliciting of contributions and campaigning;" . . .*

For clarity, the list 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 electors' personal information applies to any person or entity who receives and examines the lists of electors in printed or electronic format or on data storage devices and applications.

Table 1 – Authorized Use of the List of Electors provides an overview of the authorized uses of the list of electors to each authorized recipient. Relevant sections of the *Election Act* have been noted where applicable.

Product	Authorized Recipients	Authorized Use	Section of the Act
Official List of Electors	• Registered Political Parties • Registered Candidates	For electoral purposes only which include communicating with electors, soliciting contributions and campaigning For clarity, the list shall not be used for any purpose that is not for electoral use , including but not limited to: - Commercial use - Selling of information - Personal use	62(2) 129 (1)(a)
Strike-off information	• Registered Political Parties • Registered Candidates		65 (5) 129 (1)(a)
Post-Election records of vote	• Registered Political Parties		65 (6) 129 (1)(a)

Section 4: Requirements for Access and Use of Electors' Personal Information

Elections PEI requires registered political parties to develop and implement a privacy policy to ensure that its candidates, members of the Legislative Assembly, employees and agents comply with the restrictions on the use of information from the lists of electors under Section 62(2) of the *Election Act*. The policy must include the privacy requirements outlined in these Guidelines.

A template privacy policy for registered political parties is provided in **Appendix A** and a template privacy policy for independent candidates is provided in **Appendix B**.

The Chief Electoral Officer may refuse disclosure of the lists of electors to registered political parties, and registered candidates whose policy does not comply with the requirements stated in these Guidelines and in the Election Act, until such a time that the policy has been brought into compliance.

Filing Requirement for Privacy Policy

The privacy policy must be signed by the Leader of the Party, or Independent Candidate and the Official Agent. Once signed and submitted, the privacy policy remains a standing policy subject to the following:

- Any updates to the template privacy policy provided in this document
- Any changes to party leadership or official agent (if applicable)

Above mentioned changes will require the privacy policy to be updated and re-submitted to Elections PEI within 30 days of said changes.

Candidates who are not members of a registered political party are also required to complete a privacy policy. The candidate must submit their written policy with Elections PEI as part of their candidate registration package before being provided the Official List of Electors.

Use of Information Restrictions

The *Election Act* requires that the use of information, directly or indirectly, from the list of electors is restricted to

- Use by a registered party/ member of the party, or
- Member of Legislative Assembly, or
- A Registered Candidate

For the purpose of communicating with electors, soliciting contributions and campaigning.

For clarity, the list shall not be used for any purpose that is not for electoral use , including but not limited to:

- Commercial use
- Selling of information
- Personal use

Written Acknowledgements

A political entity must only disclose information with authorized recipients. Prior to disclosure, all authorized recipients with whom information is being shared from the permanent register must sign a written acknowledgement of these use restrictions.

Each authorized recipient must complete a written acknowledgement to indicate that they:

- understand the limits on use and disclosure of the lists;
- understand the importance of protecting electors' personal information on the lists;
- undertake to protect the confidentiality of that information;
- will use the information only for the purposes set out in the Election Act; and
- will return the lists on completion of the task for which the lists were provided to the party or candidate, as applicable. A template Written Acknowledgement is provided in **Appendix C**.
- be included in the Distribution Tracking Form available in **Appendix D**.

All signed written acknowledgements must be returned to the Campaign Manager or Official Agent who shall retain a copy for 120 days after Election Day. All documents must be available for inspection by the Chief Electoral Officer upon request.

Stakeholder Distribution Tracking

When a political entity provides a copy of information from the permanent register, or electoral products to anyone, in addition to obtaining the written acknowledgement, the political entity must also track the following information:

• date of distribution;
• who the information was provided to;
• type of document (e.g. electronic or paper copy of the list of electors)
• confirmation that the written acknowledgment has been signed; and
• confirmation of the date the copy was returned to the political entity or a certificate of destruction. A distribution tracking form must be completed for electoral products distributed during an electoral event.

A template Electoral Event Distribution Tracking Form for electoral products can be found in **Appendix D**

Filing of Distribution Tracking Form and Electoral Products

During electoral events (by-elections and general elections), registered political parties and registered candidates must maintain an electoral event distribution tracking form and submit the form with Elections PEI within 10 days after Election Day.

Section 5: Additional Privacy Requirements

In addition to the restrictions on use and reproduction of electors' personal information, to help political entities protect the information from the permanent register and electoral products, Elections PEI requires political entities to implement the following privacy safeguards outlined in these Guidelines through the party or candidate's policy, as applicable.

These safeguards provide a framework to protect the privacy of the electors' personal information contained in the registers and the lists during their use, how to dispose of the information after it has been used, and what to do if a copy of the information is lost or stolen.

The political entity must:

- provide clear direction to all authorized recipients regarding the proper use of the information obtained from the permanent register and electoral products;
- 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;
- limit the number of people who have access to reduce the chances of a privacy breach;
- ensure that the electoral products are kept secure when not in use by storing the electronic copy on a secure, password-protected computer; keeping paper copies in locked filing cabinets. Passwords and keys should be strictly controlled by the person responsible for privacy safeguards;
- ensure that all authorized recipients understand the importance of protecting the privacy of electors' information; and
- obtain from each authorized recipient a written acknowledgement that the individual will abide by the restrictions on the use of electors' personal information (see template in **Appendix C**).

Breach of Information

If a copy of an extract from the permanent register or electoral products are lost or stolen, electors' personal information in the products might be used for unauthorized purposes. Loss or theft therefore constitutes a potential 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 loss or theft to the Chief Electoral Officer

Safe and Secure Disposal of Electors' Personal Information

All political entities must dispose of electors' personal information in a safe and secure way once its use is no longer authorized. To prevent unauthorized parties from accessing personal data, it is important to use care in the disposal and destruction of electors' personal information. Reasonable steps must be taken to protect the security and confidentiality of electors' personal information that is to be destroyed, including protecting its security and confidentiality during its storage, transportation, handling and destruction.

The following provides the requirements for political entities on how to dispose of electors' personal information in a safe and secure manner:

1. Methods used must ensure that personal records cannot be reconstructed. Printed copies of documents must be properly shredded and electronic data must be permanently erased using methods that prevent the restoration of such data.

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).

Secure Disposal Documentation

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

- 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.

Personal information pertaining to the record being destroyed must not be included in the disposal record.

A template secure destruction form for electoral products can be found in **Appendix E**

If the political entity has an external company provide secure destruction services, a Certificate of Destruction must be provided by the shredding company and submitted by the political entity along with the secure destruction documentation.

Requirements of Service Provider retained to Destroy Electors' Personal Information

If selecting a service provider to securely destroy electoral products containing elector's personal information, the political entities must set out the responsibility of the service provider for the secure destruction of the records involved. The political entity must also specify how the destruction will be accomplished, under what conditions and by whom.

The political entity must require a certificate of destruction to be issued by the service provider upon completion. The certificate of destruction must include:

- the records that are being destroyed
- the date, time and location of destruction
- the method of destruction
- the name and signature of the service provider representative pertaining to the records being destroyed must not be included in the disposal record.

Section 6: Review and updates to Guidelines and Privacy Policy

The Guidelines for the Use of Electoral Products and template Privacy Policies may be reviewed and updated periodically by Elections PEI. Any updates/changes made will be communicated with all registered political parties.

Appendix B - Template Policy for Independent Candidate

Section 1: Scope of Policy

This policy applies to [ ] and any person or entity representing or working for the candidate on a paid or unpaid basis.

Section 2: Restrictions on Use

Information obtained directly or indirectly, from the Permanent Register of Electors for PEI or from a List of Electors through [ ] must not contravene section 129.1 of the *Election Act*, and be used only for electoral purposes including:

- communicating with electors
- soliciting of contributions
- campaigning

129.1 Offences, use of list of electors

"Every one is guilty of an offence who uses all or part of a list of electors for any purpose unless the list or part of the list is used

(a) by a registered party, a member of such a party or a member of the Legislative Assembly for the purpose of communicating with the electors, including the soliciting of contributions and campaigning;" . . .

For clarity, the list shall not be used for any purpose that is not for electoral use , including but not limited to:

- Commercial use
- Selling of information
- Personal use

Section 3: Requirement for Written Acknowledgements

Any person or entity who has obtained information, directly or indirectly who are authorized recipients through [ ] may only disclose it to others after obtaining their written acknowledgement that they are bound by the restrictions on use in section 129.1 of the *Election Act*, as reproduced in section 2.0 of this policy.

All signed written acknowledgements must be returned to the Campaign Manager or Official Agent who shall retain a copy for 120 days after Election Day. All documents must be available for inspection by the Chief Electoral Officer upon request.

Section 4: Tracking of Distribution

In providing any individual or entity with a copy of information from the List of Electors, the following information must be tracked:

- The date of distribution,
- Who the information was provided to,
- How the information was provided (e.g. type of document, electronic/paper copy of List of Electors etc.)
- Confirmation that the written acknowledgment has been signed, and
- Confirmation of the date the copy is returned

The Campaign Manager or other designate shall be responsible for maintain the Tracking of Distribution Form and submitting it to the Chief Electoral Officer within 10 days of Election Day.

Section 5: Breach of Information

In the case of a breach of information from the Permanent Register or an extract of the Register for a specific electoral district, the following procedures must be followed:

- the breach should be contained immediately and the source of the breach identified.
- the circumstances that that led to the incident must be documented.
- internal policies, processes and procedures must be reviewed to prevent future incidents.
- the loss or theft must be reported in writing to the Chief Electoral Officer within 24 hours of the discovery of the breach.
- Within 10 days of the breach, a report detailing the breach of information and any remediation taken.

The Campaign Manager or other designate shall be responsible for overseeing any breach of information.

_____

Signature of Independent Candidate

_____

Date

Appendix C – Template Written Acknowledgement

Last Name:	**Given Name:**	**Telephone:**
Civic Address:		

In accordance with section 129.1 of the *Election Act*, I acknowledge the following regarding the information I obtain directly or indirectly from the List of Electors or Permanent Register, whether the information obtained is in printed or electronic format or examined in either format without obtaining a copy:

☐ I have read the written acknowledgement and agree to the privacy policy

☐ I will only use such information for electoral purposes including:

- Communicating with electors
- Soliciting contributions
- Campaigning

☐ I will only disclose such information to another person if the person is authorized and only after obtaining their written acknowledgement that they are bound by these restrictions.

_____

Electoral District Name

_____

Signature of Person making acknowledgement

_____

Date

Appendix D – Template Electoral Products Distribution Tracking Form

Electoral District :

Candidate Name:

Date of Distribution	Distributed To:	Electronic Copy	Printed Paper Copy	Official List of Electors	Strike-off information	Post-Election records of vote	Written Acknowledgement Completed (**Appendix C**)	Date Returned

Completed Appendix D must be submitted to the Chief Electoral Officer within 10 days following Election Day

Campaign Manager

Campaign Manager Signature

Date

Appendix E – Template Electoral Event Secure Destruction Form

<table>
<tr><td>Electoral District:</td><td colspan="2">Candidate Name:</td></tr>
<tr><td>Name of individual or Company who securely destroyed electronic or paper copies</td><td colspan="2"></td></tr>
<tr><td>Date of secure destruction</td><td colspan="2"></td></tr>
<tr><td>Time of secure destruction</td><td colspan="2"></td></tr>
<tr><td>Location of secure destruction</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Types of documents securely destroyed (Official List of Electors, Strike-off Information)</td><td>Paper Type</td><td>How many copies were destroyed?</td></tr>
<tr><td>Electronic</td><td>How many copies were destroyed?</td></tr>
<tr><td rowspan="2">Method of secure destruction</td><td colspan="2">Paper:</td></tr>
<tr><td colspan="2">Electronic:</td></tr>
<tr><td>Signature of Individual or Company representative who destroyed electronic files or paper copies</td><td colspan="2"></td></tr>
<tr><td>If applicable, Certificate of Destruction provided by shredding company</td><td>Yes ☐</td><td>No ☐</td></tr>
</table>

If applicable, attach a copy of the Certificate of Destruction provided by the Shredding Company and submit to Elections PEI

_____ Date

_____ Candidate/Delegate Signature