GENERAL

April 2026

Political campaign activity

This guidance complements the Political Campaign Activity Code of Practice[1] (the Code), developed jointly with Elections BC. Although the Code was developed for, and with input from, provincial political parties, the principles and the guidance found in this document and the Code are applicable to campaign activity at any level, including referendum and recall campaigns. For information or guidance on electoral laws or the *Election Act*, individuals should contact Elections BC.

Purpose of this guidance document

This guidance is designed to provide best practices for political organizations – including political parties, riding associations, candidates, campaign staff, and volunteers – and their handling of personal information as part of the campaign process. BC's *Personal Information Protection Act* (PIPA) applies to the collection, use, and disclosure of "personal information" by political parties in British Columbia.

Political organizations play an integral role in a well-functioning democracy through their direct engagement with voters. This engagement is a critical component of our democratic system and typically entails collecting and using voters' personal information. At the same time, the Supreme Court of Canada has recognized that "the protection of personal privacy is also a basic prerequisite to the flourishing of a free and healthy democracy."[2]

Significant developments in technology over the years means political organizations have more tools at their disposal when conducting political campaigns. For example, predictive modeling tools and AI systems scan and analyze large datasets to help identify demographic segments and fine-tune messaging. AI-enabled chatbots communicate directly with voters, and automated voice broadcasting systems distribute pre-recorded messages to segmented voter lists at scale. Digital advertising ecosystems enable advanced microtargeting practices, such as geofencing, where advertisements are delivered to mobile devices detected within a defined geographic area, such as a particular neighbourhood or event location. These technologies can raise heightened privacy risks, particularly where sensitive characteristics are inferred or where individuals are unaware of how targeting decisions are made.

Robust engagement and protecting privacy working together can strengthen and build trust in our political system. It is the reason the OIPC has focused on the issue of campaign activities since 2019, including Investigation Report P19-01[3] that reviewed the activities of political parties against BC's privacy laws in detail. A list of several OIPC publications relevant to political organizations can be found at Appendix A.

[1] Political Campaign Activity Code of Practice (March 2022).
[2] *R. v. Jones*, 2017 SCC 60 at para 38.
[3] 2019 BCIPC 07, *Full Disclosure: Political parties, campaign data, and voter consent* [Full Disclosure].

Collection, use and disclosure of personal information

PIPA governs how political organizations collect, use and disclose personal information within British Columbia. It applies not just to provincial political organizations, but also to federal political organizations in their operations in British Columbia.[4]

Personal information is information about an identifiable individual.[5]

In most circumstances PIPA requires that personal information be collected with the consent of individuals, and only for purposes that a reasonable person would consider appropriate in the circumstances. In some cases, organizations may collect personal information without consent - but only when authorized by PIPA or another law such as the *Election Act*.

Political organizations may collect personal information in three ways:

1. With the **explicit consent** of the individual;
2. With **implicit consent**, when the collection is voluntary and the purpose for the collection would be obvious to a reasonable person; or

Types of consent

Explicit consent is a direct and understandable question asking for permission to collect, use, or disclose personal information.

Implicit consent is where there is no direct question, but permission is assumed from the circumstances. For example, by providing a political party with your email address so they can contact you to arrange a ride to a polling place on election day, you are implicitly consenting to the use of your information for that purpose.

However, you may not wish to be signed up for the mailing list of that political party and receive weekly updates of their activities.

Such secondary uses or disclosures require explicit consent. The party cannot rely upon the implicit consent you gave for the purpose of arranging a ride to authorize a secondary use such as sending you updates on their activities.

[4] *Liberal Party of Canada v The Complainants*, 2024 BCSC 814 (CanLII), appeal to BCCA pending.
[5]This includes inferred information about individuals derived from other sources of information, such as predictions about an individual's age, sex, supporter score, as well as associated demographics, such as their average education, income, and number of people in their household. See Full Disclosure at pgs 31-34.

3. Without consent, as authorized by an enactment, such as the *Election Act*[6] or a provision of PIPA that permits collection without consent, such as from public sources of information. [7]

Political organizations may use or disclose collected (or inferred)[8] information:

1. With the **explicit consent** of the individual;
2. With **implicit consent**, when the collection is voluntary and the purpose for the use or disclosure would be obvious to a reasonable person; or
3. Without consent, as authorized by an enactment, such as a provision of PIPA that permits use or disclosure without consent.

In all but the most obvious situations, political organizations should be transparent about and obtain explicit consent for their activities, including internal practices, such as analytical modelling to infer information about and predict the behaviour of individuals. Individuals must be able to understand what information political organizations collect and the way that information is used.

In most cases, PIPA requires both consent and notification to collect personal information. For consent to be valid under PIPA, it must be meaningful. Political organizations should therefore obtain consent according to the following key principles:

- explain the nature, purpose, and consequences of what the individual is consenting to;
- allow the individual to acquire more details about what they are consenting to;

Sample notification statement

By providing your name and email address you are consenting to the collection of your personal information by [political organization] for inclusion in our voter database. The personal information you provide may be combined with information we collect from other sources and will be used to engage with you as a voter in current and future political campaigns. For example, we may contact you to let you know of an event happening in your neighbourhood or to remind you to vote on election day.

We collect your personal information only with your consent, except as otherwise permitted under British Columbia's *Personal Information Protection Act* (PIPA). We do not sell your personal information and will only disclose your information to third parties as permitted under PIPA.

[6] This includes full name, home address, mailing address, electoral district and initials, and during an election may include voter participation data which identifies who voted in the most recent election along with their voting area code, voting card number and voter number. See Full Disclosure at pgs. 12-13 for more information.
[7] S.12(1)(e). See text box on page 4.
[8] Inferred information created by an organization is still personal information and any use or disclosure of that information must be authorized under PIPA.

- provide the individual with clear "yes" or "no" options;
- consider the individual's perspective;
- make consent a dynamic and ongoing process; and
- be prepared to demonstrate compliance with PIPA.[9]

PIPA requires that individuals are notified before or at the time of collection in a way that provides the individual with enough information to understand the purpose of the collection, as well as the contact information of an employee or officer of the organization who is able to answer the individual's questions.[10]

Political organizations should use the following best practices when drafting their notification statements:

- communicate clearly and directly about what personal information the political organization intends to collect and why;
- use plain language that avoids jargon and is understandable to individuals who are not members of political organizations;
- commit to proactively notifying individuals before the political organization changes how it treats their personal information;
- inform individuals if the political organization uses an artificial intelligence system, such as an automated chatbot, to interact with them;
- clearly describe how any individual voter profiling or inferred information is created and used; and
- be accountable and ready to inform individuals of whom they can contact if the individual has more questions.

Consent must be obtained for the collection of any personal information from social media websites, as they are not a "prescribed" source of personal information (see text box). For example, a political organization does not have implicit consent to "scrape" the personal information (such as name,

Public sources of information

PIPA allows organizations to collect information from "prescribed" sources without the consent of the individual the information is about. Section 6 of PIPA's Regulation sets out what the "prescribed" sources are. They include telephone directories, professional directories, government registries, and electronic publications like newspapers. However, they do not include social media sites. See Guide for organizations collecting personal information online.

[9] OIPC Guidance Document : Obtaining Meaningful Consent <https://www.oipc.bc.ca/guidance-documents/2255>
[10] See Section 10(1) of PIPA.

profile information, gender, relationship status, or photos) of individuals who "like" content posted by the organization to populate a database.

Under PIPA, individuals may withdraw their consent at any time.[11] This means that if consent is withdrawn, political organizations must cease to collect, use, and disclose the individual's personal information, except for the information in the voters list for an electoral purpose, as authorized by the *Election Act* or doing so would frustrate a legal obligation.[12] Political organizations should have processes in place to receive, process, and implement the withdrawal of consent.[13]

Reasonable purposes

Consent, whether explicit or implicit, is only one part of the equation for the processing of personal information by political organizations. It is important to understand that, regardless of consent, organizations may collect, use, and disclose personal information only for the purposes that a reasonable person would consider appropriate in the circumstances.[14]

In the context of campaign activity, purposes likely to be reasonable typically relate to voter engagement and may include:

- assessing political opinions;
- communicating about policies, events, and opportunities for engagement;
- fundraising, conducting surveys, and organizing petitions;
- communicating about political goals and policies via social media; and
- engaging in "get-out-the-vote" operations on election day.[15]

[11] S. 9.
[12] See s. 9(5).
[13] S.35(2) also requires organizations to destroy the personal information of an individual as soon as it is reasonable to assume that the retention of it no longer serves its intended purpose and retention is no longer necessary for legal or business purposes.
[14] Ss. 11, 14, 17.
[15] Council of Europe, Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108), *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (November 2021) <https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72>

Examples of purposes unlikely to be reasonable include:

- scoring or profiling individuals' political beliefs or behaviours, especially if done without the knowledge of the individual;[16]
- any purpose requiring collection, use or disclosure of biometric information (for example, digital faceprints to verify candidates' identities during nomination races);[17]
- communicating with and collecting voters' information using an automated system purporting to be from a candidate or campaign volunteer where the voter may be unaware they are communicating with a robot.[18]
- inferring, without consent, additional personal information from already collected personal information, such as guessing an individual's age, gender or ethnicity from their name;[19]
- collecting indirectly, during doorstep campaigning, information about members of a household other than one with whom a political organization directly converses, or recording observations or inferences from what is visible (for example, recording that kids toys or religious symbols are visible);
- collecting and using personal information from social media beyond what is needed to respond to individuals interacting with a political participants page, such as linking email addresses with social media profiles, collecting information such as "likes" or shares of content, or sharing identifiers with social media for the purposes of building lookalike audiences[20];
- exploiting vulnerabilities in groups of people or individuals to materially distort behaviour (for example an action that has the effect of limiting or discouraging individuals from voting);
- impersonating candidates or election officials;
- using personal information collected in a campaign to identify supporters and appoint them to public positions in the event the campaign is successful; and
- using facial recognition technology to identify supporters at a campaign rally.

[16] Full Disclosure, Recommendation 7: "All political parties should be transparent about how they profile voters."
[17] For helpful information about how facial recognition technology (FRT) works, see Joint Special Report No. 2, *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector* (June 2021) pg. 12.
[18] *Code of Practice* point 6.
[19] Full Disclosure pg. 22. This creation of new personal information, even through inference, is still the personal information of the individual it is about and requires consent.
[20] Full Disclosure pg. 21.

The above examples are not exhaustive and are intended only to illustrate the general parameters of reasonable purposes. The reasonableness of a given purpose depends upon the particular circumstances of each case; a political organization should not rely upon the examples provided without independently assessing how it intends to treat personal information.

Privacy Management

Political organizations must protect personal information in their custody or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.[21]

A good way to ensure this is to have a robust privacy management program in place well before busy campaign periods helps minimize the risk of a breach or other harms. Political organizations should, at minimum, follow a privacy management program that includes:

- maintaining a privacy policy that is open and transparent with individuals about how their personal information is collected, used, and disclosed as well as protected;
- providing reasonable security for personal information under their custody and control, including any use of personal devices;
- creating and maintaining a personal information inventory;
- conducting risk assessments on their activities, including consideration of the likelihood of information incidents and possible mitigation methods;
- training employees and volunteers to understand their obligations under both the *Election Act* and PIPA;
- retaining information only as long as needed for business or legal reasons, or when the purpose for which it was collected is no longer served;
- securely destroying all personal information, including out-of-date and irrelevant personal information;
- auditing access controls to personal information;
- role-based access and withdrawing access from individuals who no longer have a business need to access the personal information; and
- ensuring organizations contracted to provide services to the political organization adhere to the organization's standards for security and handling of personal information.

[21] S.34.

PIPA also requires that political organizations provide individuals with access to their own personal information, subject to limited exceptions.[22] In response to a request, political organizations should provide all of the requestor's personal information under their control, and inform the requestor about the ways they have used or are using the personal information and to whom the information has been disclosed.

Common campaign activities

Below are common campaign activities to which PIPA applies:

Canvassing

Political organizations collect a significant amount of information from individuals either through direct face-to-face canvassing (door-knocking) or increasingly through remote and digital means.

The following four best practices should be observed when political organizations conduct direct canvassing (in-person or over the telephone):

1. Canvassers should not collect the personal information of individuals – including, but not limited to gender, religion, and ethnicity information – unless that individual has consented to its collection (for example, this means not logging perceived race or visible religious and cultural indicators into a voter database);
2. Canvassers should only collect the personal information of individuals they speak to directly and who provide that information voluntarily (for example, not inquiring about the personal characteristics of other individuals in a household or surmising information about other individuals, such as determining and recording that an individual has a physical disability due to the presence of a wheelchair ramp by the steps);
3. Canvassers should obtain express consent for the collection of personal information for a petition if that personal information is going to be used for any purpose other than the obvious purpose of promoting the issue or objective of the petition (for example, if a petition is to "save the whales" then without further consent on the form a political organization may not add an individual's information to a general database);
4. Canvassers should conspicuously provide a succinct and simple explanation of the purposes for gathering personal information at the point of collection. How this is done depends on the nature of the communication, but could be as simple as "Can we use your information to add you to our database of supporters to contact you for future campaigns and initiatives?"

[22] S.23.

Political organizations should disclose to an individual any indirect canvassing, such as the use of an automated chatbot or other artificial intelligence-powered communication tool, with a clear opt-out mechanism for future communications of that nature.

Service Providers

Political organizations, like other organizations, often use service providers to assist them in achieving their goals. Given that political organizations collect, use, and disclose large amounts of often sensitive personal information, special care should be taken when using third-party tools, services, or software. Under PIPA, organizations are responsible for personal information both in their custody *and* under their control. If a political organization is using a service provider, such as an AI service provider, the organization is likely still in control of information, even if the service provider has custody of it. Below are some important considerations for political organizations when engaging service providers:

- beware of derivative use or broad licencing terms in software that give service providers unlimited access to user data, which may then be sold, used or disclosed to third parties in a way that is inconsistent with PIPA;
- particularly sensitive information, like a biometric face scan or political beliefs, require a higher degree of protection and great care should be taken if using a third party to process that information;
- free does not mean there is no cost; service providers that provide a free service, such as an email or cloud-based document sharing platform, often make money from user information, for example by selling the information itself or using it to improve their own products; and
- organizations should avoid service providers with poor track records on data security.

Conclusion

Political organizations are an integral part of our democracy system. They need to collect, use and disclose large amounts of our personal information to function within that system. At the same time however, the misuse or failure to protect that personal information erodes trust in political campaigning. Beyond the social harms, individuals or organizations who breach their obligations under PIPA could face serious consequences, including reputational damage and civil or administrative liability.

Political organizations must commit to collecting, using, and disclosing individuals' personal information only where authorized to do so. The most effective ways of lowering risk are to minimize the amount of personal information collected and to implement strong protections for any personal information that is collected. By aligning their practices with this guidance, political organizations will help ensure their actions will be trusted by voters and contribute to strengthening of democratic processes.

Appendix A

Investigation Report F13-04, *Sharing of Personal Information as part of the draft multicultural strategic outreach plan: Government British Columbia and the BC Liberal Party*

Obtaining Meaningful Consent, Guidance Document (May 2018)

Investigation Report P19-01, *Full Disclosure: Political parties, campaign data, and voter consent*

Privacy management program self-assessment, Guidance Document (March 2019)

Courtenay-Alberni Riding Association of the New Democratic Party of Canada (Re), 2019 BCIPC 34 (CanLII)

Courtenay-Alberni Riding Association of the New Democratic Party of Canada (Re), 2020 BCIPC 11 (CanLII)

Joint Special Report No. 2, *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector* (June 2021)

Conservative Party of Canada (Re), 2022 BCIPC 13 (CanLII)

Political Campaign Activity Code of Practice (March 2022)