Privacy Management Resource For Edmonton's Community Leagues

EDMONTON FEDERATION of COMMUNITY LEAGUES

EFCL.ORG

Introduction 2

Why You Need a Privacy Officer 2

Sample Community League Privacy Officer Job Description 3

Personal Information Protection Act (PIPA-Alberta) 4

Digital Privacy Act 10

Canadian Anti-Spam Legislation (CASL) 11

Links 14

Quick Reference 15

Introduction

Can you keep a secret? In fact, can you keep many? Did you know Community Leagues have a legal and moral duty to keep safe membership information like names, email addresses, and more?!

Did you know punishments for failing to keep personal information you've collected can add up to $100,000 or more? So you have options: build a splash park for your community *or* pay a fine for not keeping personal information safe. Upgrade your hall flooring *or* pay a fine for not keeping personal information safe. Construct an in-ground water cistern for your community garden *or* pay a fine for not keeping personal information safe. It's up to you.

Does this sound daunting? It doesn't have to. This resource has been created to provide Community Leagues with the information you need to meet privacy requirements.

There are three statutes leagues need to know about and comply with: *Personal Information Protection Act (PIPA-Alberta); Digital Privacy Act; and Canadian Anti-Spam Legislation (CASL).*

First things first, though. Does your league have a Privacy Officer? No? You should.

Why You Need a Privacy Officer

Privacy is a hot topic in the nonprofit world and requirements evolve over time. Think back a few years to CASL and the looming deadline to have all your email lists verified by the email recipient. Concern, and maybe a little panic, ensued as Leagues like yours made sure they were compliant and doing things correctly.

A Privacy Officer keeps up with all those changes and makes sure your league is behaving in a compliant way. Privacy Officers know the statutes and act as a reference point and real-life resource for Board Members. We all know turnover happens regularly on League boards, so a Privacy Officer can bring new Board Members up to speed and keep your League safe from breach.

Privacy Officers do NOT have to hold a Board position. On the contrary, it might be best for them to not sit on the Board. No doubt, there are people in your community right now who love this kind of governance practice and would be happy to volunteer as Privacy Officer for your league.

Privacy Officers:

- ➢ Keep current on privacy regulations and statutes
- ➢ Act as a resource for leagues to ensure compliance
- ➢ Don't have to be a Board Member

Sample Community League Privacy Officer Job Description

Community League Privacy Officers (CLPO) are responsible for the development, implementation, and adherence to the League's Privacy Policies. CLPO's also act as a privacy resource for Community League board members and general members.

Duties include:

- Developing and/or editing for efficacy the Community League's Privacy Policy;
- Implementing the Community League's Privacy Policy;
- Ensuring adherence to the Community League's Privacy Policy;
- Working with the League's Board of Directors to ensure all are aware of the relevant privacy legislation, the implications of said privacy legislation, and adherence to said privacy legislation;
- Acting as a human resource for questions or concerns related to the collection and safeguarding of personal information;
- Ensuring personal information is kept in a secure and satisfactory manner per the relevant privacy legislation;
- Ensuring personal information is disposed of in a secure and satisfactory manner per the relevant privacy legislation;
- Maintaining awareness of and adherence to any amendments to relevant privacy legislation as they relate to Community Leagues.

- Working with technical experts (if required) to secure digital privacy of personal information collected.

Qualifications:

- Acceptable criminal and police record checks.
- Familiarity with and interest in privacy legislation.
- The availability to meet with board members, members at large, volunteers, and community members to discuss privacy legislation as and when required.
- Ability to be a board resource at meetings and to other board members, as requested.
- Excellent communication skills.

Personal Information Protection Act (PIPA-Alberta)

Did you know there is a federal statute called the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which sets national standards for privacy practices? Alberta and British Columbia have both passed similar laws, known in each province as the *Personal Information Protection Act (PIPA)*. PIPEDA and PIPA are essentially the same in concept, but Alberta's PIPA speaks to our province in particular. In the context of Community Leagues, PIPA is sufficient to follow as a guiding statute for privacy and keeping personal information safe.

Alberta's Personal Information Protection Act (or PIPA) describes how organizations should handle its customers and employees' or contractors' personal information. The Act applies to organizations in general but for our purposes, we'll reference Community Leagues throughout so you have the information in a context that applies for your use.

Nonprofits, like Community Leagues, have some special rules under PIPA and we'll note those below.

What is Personal Information?

Personal information is any information that pertains to a person's identity such as name, address, email address, phone number, and the like. Your Community League collects personal information on membership cards, for example.

Consent to Collect Personal Information

PIPA is dedicated to the concept of *consent* when it comes to obtaining personal information. This means that you have been given the *right* or *authority*, if you will, to collect personal information from the person that's giving the right or authority.

The tricky part with *consent* is that it can be express (written or verbal), implied, or opted-out. PIPA works on the "reasonable person test" when it comes to consent and the general responsibilities for compliance of this Act. So, was the information collected for the specific use reasonable?

In the context of Community League membership cards, for example, it's reasonable to collect name, phone number, email address, street address, etc (the usual membership card stuff) and use that information for membership purposes. Buying or signing up for membership *implies consent* to the information being collected for the reasonable use of the League.

Sign-in sheets at AGM's, events, forums, etc also imply consent of the personal information given by those signing in. It is okay to collect personal information for newsletters, programs of your league, sports activities, and the like.

How to Collect Personal Information

Again, obtaining personal information must be for reasonable Community League purposes. Further, the degree of personal information must be reasonable for the reason you are collecting the information in the first place.

For example, would collecting annual income of your members be reasonable? Would collecting ethnicity be reasonable? Would collecting political party affiliation be reasonable? The answer is NO to all of these questions. There is no reasonable reason or motive to have any of this information that would be reasonable applied to Community League membership.

Is collecting the street address of members reasonable? Yes, because Community Leagues have physical (street level) boundaries that are mapped and it's important to ensure your members belong in your League and not the League adjacent to yours.

It's fairly simple to determine the personal information you can reasonably collect as a Community League. Ask the question: Is the information we are currently collecting reasonable for our Community League use and purposes? If yes, proceed. If no, rethink what you're collecting and why.

Here's a table to help you with a couple of examples:

Activity	Personal Information (Describe information)	Purpose (List why you need it)
Yoga class	Name Email address League membership number	So you know who's attending. To inform of schedule changes that may occur. To ensure participants are indeed members and therefore covered by League insurance for yoga class.
Potluck sign-in sheet	Name League membership number	So you know who's attending. So you know if the attendee needs a membership and that all in attendance are indeed members. (important if you have an AGLC license)

Who Gets to Know What's Collected?

The information that's been collected can be shared with anyone that needs access to it for reasonable purposes. For example, it is reasonable for your League yoga instructor to have access to the yoga program participant's information for communications purposes. It is not reasonable to publish yoga participant's personal information on the League website.

If a League member wants to know what kind of information has been collected about them, they must make that request in writing. The League then has 45 days to respond to the request.

Any edits or corrections to personal information needs to be made in writing. The League is responsible for making edits in a reasonable timeframe.

How to Keep Personal Info Safe

PIPA requires Leagues to take reasonable security measures against unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction of information. Leagues *need to have policies and practices* in place that protect personal information.

In effect, personal information has to be locked, protected, secure, and safe. Use of the collected personal information needs to be only for reasonable purposes and shared within reason. Old records, or ones that are no longer needed, must be destroyed prior to throwing out. (eg shredded) The following worksheet may guide your practices.

Source: https://open.alberta.ca/publications/6914844

Security practices

- ➔ We keep records in paper files.
  - ❑ Locked file cabinets and desk drawers protect information in paper files.
  - ❑ Keys are only provided to staff who need access to the files to perform their work.
  - ❑ Paper files are cross-cut shredded (or otherwise destroyed) before being disposed of.
- ➔ We keep records in electronic form
  - ❑ Computers are password-protected.
  - ❑ Staff must log in to access personal information.
  - ❑ Personal information is accessible only to those who need it.
  - ❑ Computers are physically secured (e.g. secured to a desk by a cable lock) and doors are locked.
  - ❑ Firewalls and anti-virus software are kept up-to-date, to protect against invasive malware.
  - ❑ Networks have adequate encryption according to current encryption standards (this will protect personal information, along with any other confidential information of your organization).

- ➔ We send or receive personal information via fax or email
  - ❑ Cover sheets are used to instruct a recipient to contact the organization if a fax is received in error.
  - ❑ Frequently used numbers are programmed into the fax machine to avoid dialling errors.
  - ❑ We call in advance of sending a fax containing sensitive information to ensure the intended recipient knows it is coming, and then to confirm the fax was received.
  - ❑ We only use secure email to send or receive personal information, especially when the information is sensitive.
  - ❑ We store personal information on portable media devices (e.g. laptops or flash drives)

- ❑ Personal information is stored on portable devices like laptops, flash drives and CDs or DVDs only when necessary; only as much personal information is stored as is necessary for the task.
- ❑ Portable media devices are password-protected and encrypted according to current encryption standards.
- ❑ Portable media devices are not left unattended and are securely locked away when not in use.

➔ Our volunteers/employees sometimes take files containing personal information home to work on.

- ❑ Our policy is to only take home records if necessary and with approval.
- ❑ Staff/volunteers must make sure the records are kept locked up and are not accessible to other household members.
- ❑ Our staff/volunteers members are aware of their obligation to protect privacy.
- ❑ Our board members, employees and volunteers receive information about their obligation to protect personal information.
- ❑ Our board members, employees and volunteers know who our privacy contact is.

➔ We accept credit or debit cards for payment

- ❑ Point of sale machines truncate, or black out, part of the credit or debit card numbers on the receipt.
- ❑ Our copies of credit and debit card receipts are shredded (or otherwise destroyed) when they are no longer needed.

➔ We post membership, team lists, team schedules, etc. on our website

- ❑ Consent is obtained to post names, photographs, and other personal information on our website.

Safeguarding tips to implement

_____

_____

_____

Sample Privacy Policies may be found here: *https://open.alberta.ca/publications/6914844*

Breach Happens - What Now?

Try as we might, there may come a time when personal information is accidentally released. Perhaps your League computer is breached or the League office is broken into - whatever the reason, when a breach happens, action must be taken.

If an actual privacy breach occurs, it is important to inform those affected. So let your members know (or those whose personal information was released) what happened, when, why, and what remedies you're taking to prevent a breach from happening again.

Further, it's imperative to inform the Office of the Information and Privacy Commissioner of Alberta.(OIPCA) The OIPCA is trained to help you move through a possible or actual breach of personal information.

Digital Privacy Act

The Digital Privacy Act was legislated to provide additional requirements under the Personal Information Protection and Electronic Documents Act. It came into effect November 1, 2015.

For Community Leagues, a summary of the amendments that are of relevance are:

1. Organizations must **record breaches** of security safeguards. So your League will need to keep a record of any and all breaches of personal information privacy. The defining factors for 'breach' are broad and include any and all breaches. For example, it could be argued that leaving a stack of completed membership cards unattended at an event (for example, at the sign-in table) could be a breach of security. In this case, the breach needs to be noted by the League in a document that notes all breaches.
2. Organizations are obliged to **notify** people in the event of a personal information data breach, as well as report to the Office of the Privacy Commissioner of Canada. However, this only must occur if it is "reasonable in the circumstances to believe that the breach creates a ***real risk of significant harm*** **to an individual**." That harm can include identity theft and humiliation, among other things. If a significant breach occurs, it's good practice to inform your members regardless of legislation. Again, we note the requirement for a "reasonable" approach, similar to PIPA.

3. Organizations can disclose personal information without the knowledge or consent of its customers/members to non-law enforcement organizations in order to investigate a breach of business contract or a contravention of a federal or provincial law, if said notifying those individuals could lead to a compromised investigation. Additionally, the same rule applies in fraud investigations, especially wherein someone has been labeled a "victim of financial abuse." So Community Leagues may have to share personal information if required for investigative purposes.
4. Community Leagues will need to ensure any third-party service or other organization (like Mailchimp, for example) have safeguards in place for the personal information provided by the League. It's important to make certain the personal information you collect is safe in all the ways you use it, including newsletter service providers, community newspaper providers, etc.

In essence, the Digital Privacy Act makes more determined note (which may be requested by the Privacy Commissioner) of what constitutes a breach of privacy, demands the requirement to keep a record of all breaches, and report significant breaches.

The Digital Privacy Act amendments take precedence over PIPA. Penalties are significant if Leagues fail to abide by this Act, so be prudent. A Privacy Officer can ensure you're in compliance.

Canadian Anti-Spam Legislation (CASL)

CASL is another piece of legislation that came into effect to create amendments to PIPA. CASL took effect in 2014 and was put in place primarily to prevent dreaded SPAM.

But what is spam? The simplest definition of spam is unsolicited email, though it can also include unsolicited text messages and software. Community Leagues must obtain consent, either implied or direct, to be able to send emails or texts to their members.

How to Obtain Consent

As mentioned before in this resource, consent can be implied or direct for the collection of personal information. However, in the context of CASL, consent has different definitions.

When it comes to CASL, consent is as follows:

- Direct Consent = the person gives you express consent to contact them via email. For example, Community League membership cards ask the question *Would you like to receive email news from your League via email.* If the response is YES, then this is direct consent. If the answer is no, then you clearly do not have consent to email this member. Another example of direct consent could be on a sign-in sheet at events or program registration forms that ask the question directly, like the membership card does.
- Implied Consent = the person gives implied consent to email them if they email you first; clearly the expectation is a response to their email, therefore consent is implied. Further, implied consent happens when people sign up to volunteer with your League or make a donation. The implication is that you will communicate with them via email to provide communications about the volunteer task or provide a receipt for a donation.

Note, if you're using email addresses that were obtained prior to 2014, you need to ensure consent to use those email addresses for League purposes.

<u>What NOT to Do</u>

Sending emails to members, volunteers, and others is a privilege, not a right. It's important to be respectful of email recipients. If someone who has previously consented to receive emails decides to rescind consent, then you need to comply with that request. Thankfully newsletter facilitators like Mailchimp have 'unsubscribe' options built into their system so Leagues don't even have to think about it. That said, ensure you are being compliant in this way.

Further, Community Leagues, while becoming more and more technically savvy, need to be aware that 'toggling' is unacceptable

under CASL. What is toggling? It is the requirement for people to need to remove consent, as opposed to offering consent. For example, those pre-checked boxes you may see on websites or emails that require you to *unclick* or receive further information from the website or sender is considered toggling. It isn't fair or legal to ask people to remove consent by pre-checking consent boxes.

Cookies, Malware, Javascript, Oh my!

CASL deems a person to have provided express consent for the installation of a computer program, if it is reasonable to believe that the person consented to the installation based on the person's conduct, and the computer program is:

- a cookie,
- HTML,
- JavaScript,
- an operating system,
- a program that is executable only through another computer program to which the user has already expressly consented, or
- specified in the regulations.

Translation: if you get to a point in your League communications where you may be requiring your members, volunteers, or others to install software to 'do business' with your league, consult with your Privacy Officer to ensure you are in compliance with CASL. This may become of importance for instances such as a volunteer treasurer installing bookkeeping software or a volunteer coach using an 'app' to keep track of rankings on a sports team, etc.

Record-keeping of CASL Consent

As you can imagine, keeping a record of consent for digital communications, like emails, is important for CASL compliance. Records can be kept via membership cards, email sign-up lists, newsletter sign-up lists, and the like. Of course, as discussed above, those records need to be safe-guarded, password protected, locked, etc.

Links

When in doubt, go to the source.

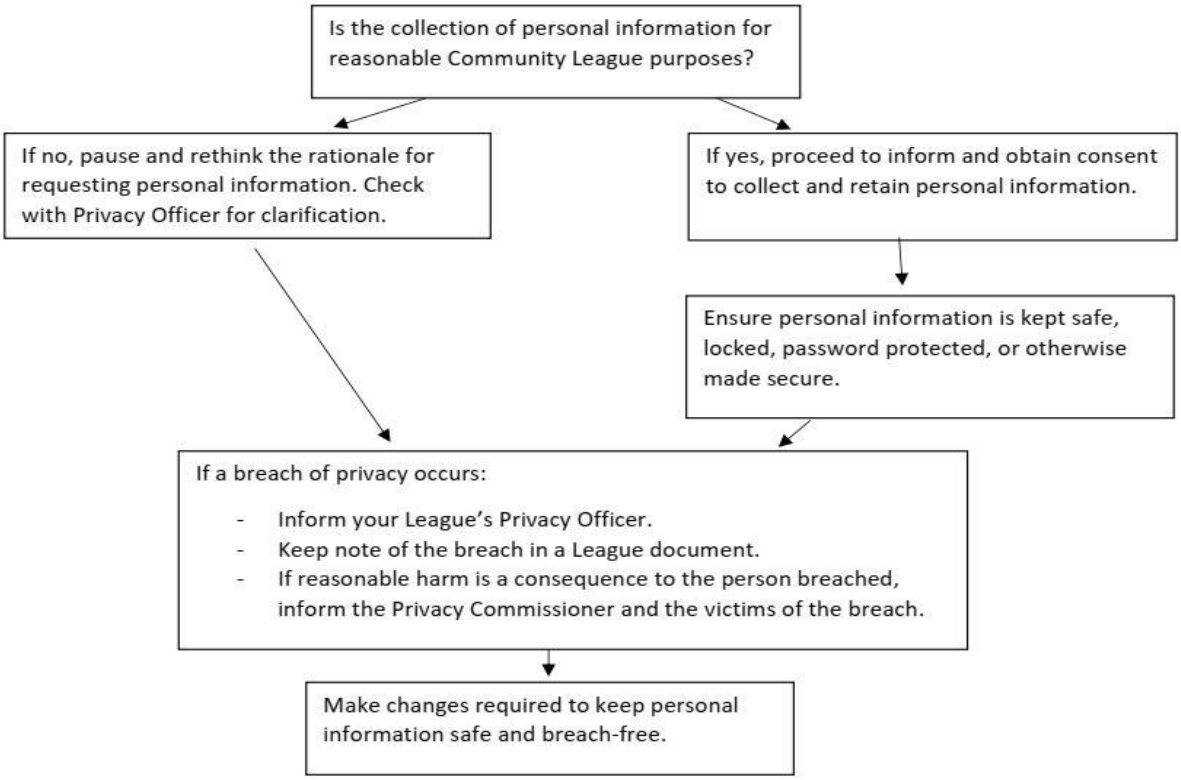
PIPA

DPA

CASL

Quick Reference

Quick Reference Sheet for PIPA and DPA Compliance



Before Sending Email Correspondence Ensure Consent

Does your League have direct consent via the person's membership card?

Has the person emailed the league?

Has the person signed up for a program, to volunteer, or made other direct contact with the league via email?

If the response is YES to any of these questions, proceed with your correspondence. If no, obtain consent.