BOYS AND GIRLS CLUBS OF CANADA

Privacy Policy

Boys & Girls Clubs of Canada

Privacy Plan

Introduction

This Privacy Plan provides guidelines for ensuring privacy of personal information provided to BGCC operations. Information about our stakeholders their names, addresses, purchasing history — is a valuable asset to our work. But unlike other assets, there are strings attached. Our members, donors and other constituents retain an interest in what we do with their personal information. Mishandling it exposes our organization to risks. It can damage our reputation in the community, lead to legal liability and fines, and destroy the trust that is the cornerstone of good relationships with our various publics. Building privacy protections into our operations will limit these risks and protect our investment in a valuable business asset — our stakeholder information.

The following report provides us with an action plan and recommendations on how to ensure our organization is secure when it comes to privacy matters.

Action Plan

Private Information Collected By BGCC

This summarizes what information we collect, who in our operations collects it, who uses it and what they use it for. This document gives you a bird's-eye view of our information practices and helps us manage training needs and on-going security issues.

Consent Practices

The summary of our Consent Practices clarifies when we assume a customer is consenting to the collection, use and disclosure of information, and when we need to provide an opt-out or get express consent.

Security Plan

The Security Plan sets out what we can do right now to improve the ways in which you safeguard our stakeholders' information. It also identifies the sensitive information you collect, so you can make sure it's given the highest level of protection.

Third Parties List

The Third Parties List identifies those companies you share personal information with so we can review the privacy practices of these firms to make sure they meet the same standards that we apply in your business.

Privacy Brochure

The Privacy Brochure helps you get the right information to our constituents so that our privacy practices are open and transparent.

Training Plan

Last but not least, the Training Plan identifies the employees who need to be trained in how to obtain consent and how to answer customer questions about our privacy practices.

Type of Information	What WE collect	Who collects it	For what reason	Who uses it	Stored by	Shared with
Contact Information	Name Address Postal Code Phone Number Email Address	Any staff “Members only” log in	To complete a sale/donation/ transaction To provide customer service To administer an awards program Partner Relationship Management to conduct Contests/Surveys Deliver goods or services Application forms Complaints	Many staff	CRM records Paper File	Partners Suppliers Third party contractors (such as a courier company or Partner Relationship Management consultant)
Member Demo graphics	Date of Birth/Age Gender Household Income	Scholarships Board support Youth conference registration Donor administration	Customer service Contests/Surveys Adjudicate application forms for scholarship Because it is required by law	Specific Staff	CRM records Paper File	Scholarship Partners
Financial Information	Payment card number Payment card expiry date Banking information	Accounting and donor management	To complete a sale/donation/trans action goods Delivery services Returns Process Application forms Transmit Funds	Specific Staff	Used then destroyed, not stored	Transmitted on the payment form
Opinions/ Interests	Member club staff satisfaction info Opinions about products and services Interests and hobbies	Donor management, scholarships and program surveys	Member service Partner Relationship Management Scholarship Application forms Complaints	Specific staff	Electronic Files Paper File	Partners
Other Information	Social insurance number Health/medical information Driver's license number Photos	Scholarships/ payroll youth conference Bank forms Promotion materials	Application forms Because it is required by law	Specific staff	Electronic File Paper File	CRA Conference Staff Bank Authorities Public

Privacy Officer
It is important that someone in our organization be responsible for implementing our privacy plan. In our organization, that individual is:

Name/Title: Owen Charters, CEO
Address: 2500 Sheppard Ave. E, Suite 400, Toronto, Ontario M2J 5B4
Phone: 905 477-7272 ext. 226
Email: privacyofficer@bgccan.com

Consent Practices
Consent is voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. **Express consent** is unequivocal and does not require any inference on the part of the organization seeking consent. **Implied consent** arises where the consent may reasonably be inferred from the action or inaction of the individual.

Express Consent:
BGCC collects the following information that is either sensitive or potentially sensitive.

- Date of birth/age
- Household income
- Payment card number
- Payment card expiry date
- Banking information
- Opinions about products and services
- Interests and hobbies
- Social insurance number
- Health/medical information
- Driver's license number
- Photos

When collecting sensitive or potentially sensitive information, we always make sure we get express consent. In other words, we must ask the customer directly if they consent to us collecting the information and/or disclosing the information to another company. For example, if you collect financial information on a scholarship application, have the member sign an application form that states that you will disclose the information to an adjudication committee; that is considered express consent. Or, if we collect medical information on a conference registration form, it is considered express consent if the person provides the information for us to use it in medical emergencies.

Express consent should be used whenever possible and in all cases when the personal information is considered sensitive.

Implied Consent:
BGCC collects the following information to complete a donation or other transaction, scholarship applications, place a special order for a customer, arrange for a delivery or process a return:

- Payment card number
- Payment card expiry date
- Banking information
- Customer satisfaction info
- Opinions about products and services
- Interests and hobbies

- Social insurance number
- Health/medical information

So long as the information collected is necessary to complete a particular action stated at the point of data collection, you can assume the customer has consented when he or she provides you with the information. (This is called “implied consent.”)

The only time we collect driver’s license information is for registering signing officers at the bank. In the future it might arise, that BGCC will collect more opinion or survey type information from the general public through our website. In each new instance, thought will have to be given to express and implied consent options.

Remember:
- You can't refuse to complete a transaction if the customer refuses to consent to the collection of information that isn't necessary to complete the transaction.
- If you decide later to use this information for another purpose, you have to go back and get the customer's consent.

Opt-Out Consent:
BGCC does not often collect information for secondary purposes, such as marketing, administering a customer loyalty program or Partner Relationship Management; however should we chose to develop a program through our website to be possible we must collect:
- Customer satisfaction info
- Opinions about products and services
- Interests and hobbies

In these circumstances, we have to give the respondent an opportunity to tell us they don't want us to use their information for that purpose. This is called an “opt-out.”

Opt-outs must be clear, easy to understand and easy for the member to do. You can have an opt-out box on a paper-based or web application form, for example, which tells members that if they don't want to receive promotional material in the mail, just check here. You may want to let the member know what they'll be missing — special deals and new product information, for example — but don't minimize, hide or obscure the opt-out. And don't make it complicated, like requiring the member to call a special phone number between certain hours. The point is to let the member decide.

Security Plan

Employee Access to Customer Information
At BGCC, we know that private protection should be collected and viewed by those who have a responsibility to administer certain tasks, therefore there are no employees in our organization who see or process information unnecessarily. By limiting the number of people who view or process information, you reduce the risk of inappropriate use or disclosure of private information.

Storage of Personal Information: Paper Files and Electronic Files
The following includes the types of information that are stored in either paper or electronic files at BGCC:

- Name
- Address
- Postal code
- Phone number
- E-mail address
- Date of birth/age
- Gender
- Household income
- Banking information
- Customer satisfaction info
- Opinions about products and services
- Interests and hobbies
- Social insurance number
- Health/medical information

It is important to take all measures possible in order to safely store our stakeholder's personal information. Information kept on the file server is protected by our password processes. Information stored on desktop hard drives or on USB keys is not similarly protected. Private information should not be stored on these devices.

Special mention needs to be made of mobile devices. Some staff choose to receive work-related e-mails on their mobile phones. Individual staff are responsible for the use and misuse of BGCC information while in their possession. It is highly recommended that personal information other than contact information, and especially sensitive information that might be received on a mobile device, be deleted immediately. The information can be properly dealt with in the secure work environment.

Paper files that contain private information are to be kept in a locked cabinet. Sensitive information should be destroyed once its intended use (adjudication of grants for instance) is complete.

Be especially careful with laptops, USB keys and electronic wireless devices. These types of devices can potentially store a large quantity of our stakeholder's personal information. All of these devices should be password protected and have the strongest form of protection possible.

Collection of Sensitive Information
At BGCC, we have some instances in which we collect information that is either sensitive or potentially sensitive. This information is collected for a specific purpose then destroyed:

- Date of birth/age
- Household income
- Payment card number
- Payment card expiry date
- Banking information
- Opinions about products and services
- Interests and hobbies
- Social insurance number
- Health/medical information
- Driver's license number

Each staff member is responsible to destroy this information once the intended use for it is finalized.

Third Parties List
At BGCC, we share some personal information with the following third party suppliers or agents:

- National Partners (ages of scholarship recipients, for instance)
- Suppliers (basic contact information for deliveries, for instance)
- Third party contractors (such as a database developer, for instance)
- Government (to issue T4s and T41s, for instance)

When we execute program partnership or sub-contractor agreements, we require our partners to adhere to strict privacy guidelines to ensure they meet the same standards that we apply to your operations. In particularly unusual circumstances, please speak with our Privacy Officer to determine if we require legal advice for specific circumstances. In all instances of dealing with third parties we want to be sure to:

- Require the third party to protect our stakeholder information;
- Give us the power to audit the third party to make sure they're complying with fair information practices;
- Make sure the third party only uses the information for the purposes set out in the contract;
- Require the third party to pass on to us any requests from customers to see their customer records.

Training
Training is absolutely essential if our privacy plan is going to be successful. Our staff are the face of our organization, both to our member clubs and to the general public. Why they're being asked for personal information or how they can opt out may affect whether or not that constituent decides to do continue working with our organization in the future.

One of the simplest ways we can make our business privacy-compliant is to make arrangements immediately to stop collecting information that is not required to run our business. The following table shows the information we have identified we need to collect in order to perform a certain action. All other requirements for private information should be carefully scrutinized and eliminated if not necessary.

Purpose	Contact	Customer	Financial	Opinions/	Other

	Information	Demographics	Information	Interests	Information
To complete a sale/order	Name Address Postal Code E-mail Address	Gender (required by CRM) •	Payment card number Banking information Payment card expiry	Customer satisfaction info Opinions about products and services Interests and hobbies	•
To complete a donation	Name Address Postal Code E-mail Address	Gender	Payment card number Banking information Payment card expiry	Customer satisfaction info Opinions about products and services Interests and hobbies	•
Marketing	Name Address Postal Code E-mail Address Phone Number	Gender Date of birth/age		Customer satisfaction info Opinions about products and services	
Member services	Name Address Postal Code E-mail Address	Gender		Opinions about products and services Interests and hobbies	Social insurance number Health/medical information
Employee Payroll	Name Address Postal Code E-mail Address	Gender			Social insurance number Health/medical information
To administer an awards program	Name Address Postal Code E-mail Address	Gender Date of birth/age •	Payment card number Payment card expiry date Banking information	Interests and hobbies	
Partner Relationship Management	Name Address Postal Code E-mail Address	Gender			
Contests/Surveys	Name Address Postal Code E-mail Address	Gender		Interests and hobbies	

Delivery of Goods	Name Address Postal Code E-mail Address	Gender Household income			
Returns	Name Address Postal Code E-mail Address	Gender			
Scholarship Application forms	Name Address Postal Code E-mail Address	Gender Household income		Opinions about services	Social insurance number
Complaints	Name Address Postal Code E-mail Address	Gender		Opinions about services	

Further Considerations:
It is important to limit the collection to only information that is necessary. If you do not need to collect information for a certain purpose, then you should limit your collection of information to what is required and necessary. Remember, limiting the collection of personal information to what is required and necessary can reduce the amount of personal information we need to store and our costs to store and safeguard that information.

How much personal information should you collect?
With new information technologies, there's a temptation to collect personal information just in case it could be useful in the future. But under privacy laws, we have to tell our constituents why we're collecting the information and then stick to that purpose. If you want to use the information for another purpose, you have to go back to the individual and get his or her permission.

Once we do collect the information, we are also required by law to keep it up-to-date, accurate and secure and to provide customers with access to it on request.

In other words, there are hidden costs and obligations involved when we collect personal information. One of the easiest and cheapest ways we can make our organization privacy-compliant is to collect only what we actually need.

Notes section in CRM
At BGCC, we have the option of recording “Notes” for any contact in our CRM database. The note field should not be populated with personal information.

When you're deciding what to collect, remember that you're obligated to make sure you're only collecting information for purposes that a “reasonable person would consider appropriate in the circumstances.” In Quebec, the requirement is that the information has to be “necessary for the object of the file.”

Photocopies of Driver's License
The only purpose in which we collect driver’s licenses currently is to provide positive identification to our bank for signing authorities this is collected in the form of a photo copy this is never kept on file.

Collection of social insurance numbers
Our organization collects employee and student social insurance numbers. The Office of the Privacy Commissioner of Canada has long held the position that the Social Insurance Number (SIN) should not be used as a general identifier and that organizations should restrict their collection, use and disclosure of SINs to legislated purposes.

Employers are authorized to collect SINs from employees in order to provide them with records of employment and T-4 slips for income tax and Canada Pension Plan (CPP) purposes.

Complaints
We have a register for complaints (new for 2011), which is in CRM, but not intertwined with contact records. This allows any staff member to record a received complaint (whether that complaint is directed to a Club or to the National office). Discretion should be used in recording a complaint by noting verbatim the complainant’s comment and not referencing the complaint in other records.

So the next step is to review the information you collect and follow the **3 Rs** — make sure it's

Reasonable, Relevant to your purpose and **Really Needed** for your business. If not, don't collect it.

How to protect the personal Information you collect?
Now that we've agreed to limit the personal information BGCC collects to what's **Reasonable, Relevant** and **Really Needed**, the next step is to make sure you keep that information safe and secure.

Under the law, we are required to use security safeguards to protect the personal information we have from things like unauthorized persons getting access to it for copying, modifying or destroying it. Federal laws also talk about protecting it from loss or theft, and Quebec laws call for safety measures that will ensure the information is kept confidential.

Keeping information secure doesn't have to be high-tech. The best protection is to limit who gets access to it on a "need-to-know" basis only.

Next, think about how sensitive the information you collect is. Generally speaking, the more sensitive it is, the better our security arrangements should be. Information about a person's health or financial situation is always considered sensitive and must be protected with higher safeguards. Therefore we use the conference management and scholarship adjudication and then the information is destroyed.

This information needs to be well protected from prying eyes.

It is also important to remember that other information may be sensitive, depending on the context. For example, the fact a person subscribes to a magazine for cancer survivors may be sensitive in some circumstances. Partner Relationship Management databases and lists may also be sensitive because they are lucrative targets for identity thieves who want access to the information so they can impersonate your customers.

Next, think about where you keep your personal information. Security can be as simple as locking a filing cabinet or restricting who has access to an office.

Finally, think about what you do with old files. As a general rule of thumb, you should only keep personal information for as long as you need to fulfil the purpose that you collected it for. After that, you should destroy it.

But take care. Canadian organizations have ended up in the news when their old files ended up in boxes on the beach or on the back of real estate pamphlets circulated in Toronto. Invest in a shredder for smaller jobs, and use a magnet to destroy any electronic files that may be stored on old equipment. If you're contracting out, make sure you use a reputable firm that will completely destroy your files.

Explain why and ask for permission
The best way to manage your privacy risks is to let your customers know why you're collecting the information and ask them for their permission.

There are times when it's obvious your customer knows why you're collecting the information and consents to it. For example, when a donor provides his or her credit card information anytime, he or she knows your business will record the card number and pass it onto the bank so you'll be paid. The customer's consent to the use of the card number for the limited purpose of payment can be

implied from the circumstances.

You indicated that you collect the following information to complete a Donation or transaction, verify a customer's credit, place a special order for a customer, arrange for a delivery or process a return:

So long as this information is necessary to complete one of the transactions listed above, you can assume your customer has consented to the collection and use of his or her personal information for that purpose. (This is called "implied consent.") But remember, if you decide later to use this information for another purpose, you have to go back and get the customer's consent.

How to respond to inquiries and complaints
Responding fairly and quickly to customer concerns is one of the fastest ways to privacy compliance. The single most important thing you can do is to make sure exactly what personal information your organization collects and why you collect it, so you can answer customers' questions.

Each of us may collect information from various stakeholders.

If a member or stakeholder wants more information about our privacy practices, make sure you know each and every privacy policy that tells members and stakeholders that is confidential or sensitive:

- What personal information you collect;
- How you use it;
- What other organizations you share it with and why;
- Who in your organization they can contact if they want to see their own records, or have questions or complaints;
- How to contact the Privacy Commissioner's office for more information or assistance.

Designing an effective brochure isn't that difficult once you know what information the customer needs. To make it easier, we'll give you a sample brochure at the end of this training session.

Third Party Suppliers or Agents
Sometimes sharing customers' personal information is just a regular part of doing business, like when a store passes on a customer's address to a courier to deliver a product. Other retailers may decide to share that information — with the customer's consent — with partners or marketers.

It's important to remember that your responsibility doesn't end when the information leaves your hands. Whenever you share personal information with a third party, it's up to you to make sure it's going to be protected.

- At BGCC, we require third party suppliers to protect your customer information;
- Give us the power to audit the third party to make sure they're complying with fair information practices;
- Use the information for the purposes set out in the contract;
- Require the third party to destroy the information once the contract is completed.