LINDEN CHRISTIAN SCHOOL – PRIVACY POLICY JUNE 2019

PERSONAL INFORMATION PRIVACY COMMITMENT STATEMENT

This Privacy Policy (the "policy") has been developed:

- To affirm our commitment to protecting the privacy, confidentiality, accuracy and security of individuals at Linden Christian School ("LCS"); and
- To document our practices concerning the collection, use and disclosure of personal information provided by individuals and organizations.

For purposes of this policy, Individuals include, but are not limited to the following categories:

- Current and former students of LCS;
- Current and former parents and/or guardians of students at LCS;
- Current and former employees and independent contractors of LCS;
- Current and former volunteers of LCS;
- Current and former members of LCS;
- Current and former board directors of LCS;
- Current and former donors of LCS; and
- Current and former applicants to LCS.

To safeguard the personal information entrusted to LCS and to comply with the Personal Information Protection and Electronic Documents Act ("PIPEDA") and any other applicable legislation, LCS is committed to the following principles:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, retention and mandatory breach reporting
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

LCS, its members, directors, officers, employees and volunteers are required to comply with the principles and the policy and will be given restricted access to personal information solely to perform the services provided by LCS.

Other persons or organizations who act for, or on behalf of, LCS are also required to comply with the principles and the Policy and will be given restricted access to personal information solely to perform the services provided for LCS.

In the event that an Individual affected by this Policy is a minor, only the minor's parent(s) and/or legal guardian must be contacted and/or consulted, as required below.

LCS has designated Diana Koldyk, Director of Finance, to be LCS's Personal Information Compliance Officer. Any inquiry, request or concern related to privacy matters should be made in writing to LCS at:

Diana Koldyk, FCPA, FCMA
Personal Information Compliance Officer
Address: 877 Wilkes Avenue, Winnipeg, MB R3P 1B8
e-mail address: dkoldyk@lindenchristian.org; telephone 204-989-6746

A copy of the policy is available at the LCS's website www.lindenchristian.org. A printed copy of the policy may be requested by mail or e-mail at the above address.

POLICY TO PROTECT PERSONAL INFORMATION

1. Accountability

1.1 Diana Koldyk is hereby appointed as the Personal Information Compliance Officer (the "Officer").

1.2 All persons, whether employees, independent contractors, volunteers, or members, board directors or committee members who collect, process, or use personal information shall be accountable for such information to the Officer.

1.3 This policy shall be made available upon request.

1.4 Personal information is oral, electronic or written information about an identifiable Individual.

1.5 Any personal information transferred to a third party for processing is subject to this policy. The Officer shall use contractual or other appropriate means to protect personal information at a level comparable to this policy while a third party is processing this information.

1.6 Personal information to be collected, retained, or used by the organization shall occur after the Officer provides written approval. This information shall be secured according to the Officer's instructions.

1.7 Any person who believes the organization uses personal information collected, retained, or used for purposes other than those that person explicitly approved, may contact the Officer to register a complaint or to make any related inquiry.

1.8 Upon receiving a complaint from any person regarding the collection, retention, or use of personal information, the Officer shall promptly investigate the complaint and notify the person who complained, about the Officer's findings and corrective action taken, if any.

1.9 Upon receiving the response from the Officer, the person who filed the complaint may, if they are not satisfied, appeal initially to the organization's Chief Executive Officer and then, secondarily, to the LCS Board of Directors to review and determine the disposition of the complaint at issue.

1.10 The determination of the Board of Directors shall be final and the Officer shall abide by and implement any of its recommendations.

1.11 The Officer shall communicate and explain this policy and provide training to all employees and volunteers who might be in a position to collect, retain, or use personal information.

1.12 The Officer shall prepare and disseminate information to the public, which explains LCS's protection of personal information policies and procedures.

2. Identifying Purposes

2.1 The Officer shall document the purpose for collecting personal information in compliance with the principles outlined herein.

2.2 The Officer shall determine the information that is required to fulfill the purposes for which the information is to be collected, in accordance with the principles herein.

2.3 The Officer shall ensure that the purpose is specified at or before the time of collecting the personal information from an Individual.

2.4 The Officer shall ensure that the information collected will not be used for a new purpose before obtaining the Individual's approval, unless the new purpose is required by law.

2.5 The Officer shall ensure that the person collecting personal information will be able to explain to the Individual the purpose of collection.

2.6 The Officer shall ensure that limited collection, limited use, disclosure, and retention principles are followed in identifying the purpose for the collection of personal information.

3. Consent

3.1 The Officer shall ensure that the Individual from whom personal information is collected, consents to this collection and to the information being used and disclosed, unless obtaining the consent would be inappropriate. Consent may be obtained verbally or in other written formats. Consent may also be obtained from an authorized representative or substitute decision-maker, such as a legal guardian or a person having power of attorney.

Personal information may be collected, used, or disclosed without the Individual's knowledge and consent in the following situations:

- When information is being collected to detect and prevent fraud;
- When the Individual is seriously ill, or mentally incapacitated; and
- When disclosure involves legal counsel, in order to comply with a subpoena, warrant or other court order, or is otherwise required or authorized by law.

3.2 The Officer shall ensure that the Individual can reasonably understand why and how the information will be used when the consent is given.

3.3 The Officer shall ensure that no condition is attached to supplying benefits, because of the organization's activities, requiring the Individual to give consent for the collection, use, or disclosure of information beyond that required to fulfil the specified and legitimate purposes.

3.4 The Officer shall ensure that express consent is obtained wherever possible and appropriate. In rare circumstances, in the Officer's opinion, implied consent might be acceptable. Implied consent occurs when the Officer can reasonably conclude that an Individual has provided LCS with consent to collect, use and/or disclose their personal information by some action they have taken.

3.5 In obtaining consent, the Officer must respect the Individual's reasonable expectations.

3.6 The Officer shall ensure that the express consent obtained from an Individual is clear and in an appropriately verifiable form.

3.7 Where appropriate, the Officer is to obtain contractual commitments from third parties to whom there has been a transfer of personal information, to ensure that the personal information is protected in accordance with relevant privacy legislation and this policy, even when in the possession of third parties.

3.8 The Officer shall ensure that the Individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The Individual shall promptly be informed of the implications in withdrawing consent. Such withdrawal would not be effective if LCS is required, by law, to collect, use or disclose such Individual's personal information, or if such collection, use or disclosure is a term of any agreement or understanding LCS has with that Individual in operating our programs. Individuals may contact the Officer for more information regarding the implications of withdrawing consent.

3.9 Should the information be disclosed for a purpose other than those outlined in the policy, then the new purpose will be documented and the Officer will obtain the Individual's consent at or before the time the information is used or disclosed.

4. Limiting Collection

4.1 The Officer shall ensure that personal information will be collected only to the extent necessary to fulfil the purposes identified. The Officer, upon request, shall specify the type of information to be collected, according to the Openness principle as defined in Section 8 of this policy.

4.2 The Officer shall ensure that information is collected only by fair and lawful means, without misleading or deceiving Individuals as to the reason for the collection of personal information.

4.3 The Officer shall ensure that the Individual understands why such personal information is to be collected.

5. Limiting Use, Disclosure, Retention, and Mandatory Breach Reporting

5.1 The Officer shall ensure that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the Individual, or as required by law, and any use of personal information shall be properly documented.

5.2 The Officer shall ensure that all personal information is destroyed, or erased as soon as the purpose for which it was collected is no longer relevant, or as permitted by law. There shall be an annual review of the need to continue retaining personal information. Except as required to be retained by law, all personal information shall be deleted or erased no later than seven years after the purpose for which it was collected, has been completed.

5.3 The Officer shall ensure that all use, disclosure, and retention decisions are made in light of Sections 2, 3, and 9 of this policy.

5.4 The Officer may disclose an Individual's personal information to a third party where such disclosure is required in order for LCS to comply with legal or regulatory requirements as authorized by law.

5.5 The Officer will report breaches to the Office of the Privacy Commissioner of Canada and notify affected Individuals (and possibly third parties) when:

- The organization experiences a breach of security safeguards involving personal information under its control; and
- if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an Individual.

5.6 In the event of a breach of security safeguards involving personal information to an Individual, or group of Individuals, then the Officer must report the breach to the Privacy Commissioner of Canada. Thereafter, the Officer must notify the affected Individual(s) of those breaches, and keep a record of all breaches. The types of breaches to be reported are those that pose a real risk of significant harm to individuals. This includes, but is not limited to:

- bodily harm;
- humiliation;
- damage to reputation or relationships;
- loss of employment;
- business or professional opportunities;
- financial loss;
- identity theft;
- credit records; and
- damage to or loss or property.

5.7 The Officer is required to keep records of all breaches of security safeguards of personal information, whether or not the breach constitutes a real risk of significant harm.

5.8 At a minimum, the Officer must keep the following information:

- the date or estimated date of the breach;
- general description of the circumstances of the breach;
- the nature of information involved in the breach; and
- whether or not the breach was reported to the Privacy Commissioner of Canada, and whether or not individuals were notified.

5.9 The record must include an account of the reporting and notification requirements, and the information gathered in assessing whether or not such breach was a real risk of significant harm. Such records are required to be kept on file for two years.

5.10 After complying with the above, unless otherwise prohibited by law, the Officer must notify the Individual as soon as possible of the breach, provided the breach has been classified as a real risk of significant harm. In notifying the Individual, it must include the following information:

- a description of the circumstances of the breach;
- the day on which, or period on which, the breach occurred or, if neither is known, the approximate period;
- a description of the personal information that is the subject of the breach to the extend that the information is known;
- a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- contact information that the affected individual can use to obtain further information about the breach.

5.11 The Individual must be notified directly, in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances.

5.12 In the event that direct notification may cause further harm to the affected Individual, cause undue hardship for LCS, or such contact information of the Individual does not exist, the Officer may notify the Individual indirectly, by public communication, such as an advertisement, or a message on the LCS website.

6. Accuracy

6.1 The Officer shall reasonably ensure that the personal information is accurate, complete, and up to date, as deemed necessary, taking into account the Individual's interests, and to minimize the possibility that inappropriate information might be used to make a decision about an Individual. The Officer may contact Individuals to verify the accuracy of the information.

6.2 The Officer shall ensure that the organization does not routinely update personal information, unless it is necessary to fulfil the purposes for which the information was collected.

6.3 The Officer shall ensure that personal information used where necessary on an ongoing basis, including information that is disclosed to third parties, will generally be accurate and up to date, unless limits to the requirement for accuracy are clearly set out.

7. Safeguards

7.1 The Officer shall ensure that the organization has security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, destruction or modification, and shall do so regardless of the format in which the organization holds the information.

7.2 Depending on the information's sensitivity, the Officer may permit reasonable discretion regarding the information that has been collected, such as the amount, distribution, format, and the method of storage. A higher level of protection shall safeguard more sensitive information.

7.3 The Officer shall ensure that the protection methods include:

- physical measures, for example, locked filing cabinets and restricted access to offices;
- organizational measures, for example, security clearance and limiting access on a "need-to-know" basis; and
- technological measures, for example, the use of passwords and encryption.

7.4 The Officer shall ensure that all employees and volunteers know the importance of keeping personal information confidential. Further, the Officer shall ensure the protection of personal information disclosed to third parties by contractual or other means stipulating the purposes for which it is to be used, and the necessity to provide a comparable level of protection.

7.5 When personal information is disposed of or destroyed, the Officer shall ensure that care is taken to prevent unauthorized parties from gaining access to such information.

7.6 The Officer will ensure that security practices are controlled, monitored, and reviewed on a regular basis. Current technologies will be employed to ensure that confidentiality and privacy are not compromised.

8. Openness

8.1 The Officer shall ensure that the organization is open about its policies and practices regarding the management of personal information. The policies and information about the related practices shall be available to all employees and volunteers.

8.2 The Officer shall ensure that the information available shall include:

- the name or title and address of the Officer who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

- the means of gaining access to personal information held by the organization;
- a description of the type of personal information held by the organization, including a general account of its use;
- a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
- what personal information is made available to related organizations (e.g., organizations that are affiliated).

8.3 The Officer shall ensure the information provided according to 8.2 is available either in a brochure at the locations the organization operates, online, or by mail.

9. Individual Access

9.1 The Officer shall ensure that upon request the organization shall inform an Individual whether the organization holds their personal information. If possible, the organization shall provide the source of the information. The organization shall allow the Individual access to this information except in circumstances where disclosure is prohibited by law or contrary to the purpose for which the information is gathered. The organization may choose to make sensitive medical information about its employees or volunteers available through a medical practitioner. The organization shall also account for the use that has been made or is being made of this information and give an account as to the third parties to whom it has been disclosed.

9.2 The Officer may require the Individual requesting their personal information to give sufficient information permitting the organization to provide an account of the existence, use, and disclosure of personal information. Information shall be used only for the purpose for which it was obtained.

9.3 If the organization has supplied personal information about the Individual to third parties, the Officer shall ensure that an attempt is made to be as specific as possible. If the list of the organizations to which the organization has actually disclosed information about an Individual is unclear, the organization shall provide a list of organizations to which it might have disclosed information about the individual.

9.4 The Officer shall ensure that the organization responds to the Individual's request within a reasonable time and at minimal or no cost to the Individual. The requested information shall be made available in a generally understandable form. For example, the organization shall explain abbreviations or codes it uses to record information.

9.5 The Officer shall ensure that when an Individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. When appropriate, the amended information shall be transmitted to third parties having access to the information in question.

9.6 In certain situations, the Officer may not be able to provide access to all of the personal information held about an Individual. In such a case, the Officer will provide the reasons for denying access upon request. For example:

- if doing so would likely reveal personal information about another Individual or could reasonably be expected to threaten the life or security of another Individual;

- if doing so would reveal any of the organization's confidential information;
- if such disclosure is prohibited by law;
- if the information is protected by solicitor-client privilege;
- if the information was generated in the course of a formal dispute resolution process; or
- if the information was collected in relation to a breach of a federal or provincial law.

10. Challenging Compliance

10.1 The Officer is authorized to address a challenge concerning compliance with the above principles.

10.2 The Officer shall develop procedures to receive and respond to complaints or inquiries about the policies and practices regarding the handling of personal information. The compliance procedures shall be easily accessible and simple to use.

10.3 The Officer shall inform Individuals inquiring about lodging complaints that relevant complaint procedures exist.

10.4 The Officer shall investigate all written complaints. If a complaint is found to be justified, the Officer shall take appropriate measures, including, if necessary, amending the policies and practices.