



Privacy Policy

Preamble

As image bearers, we recognize that we are uniquely created with gifts and skills and we should treat one another with respect. This respect includes how we collect and manage personal information of others. The *Personal Information Protection and Electronic Documents Act* (“*PIPEDA*”) is federal privacy legislation that also applies to the collection, use and disclosure of personal information by private sector organizations in Ontario in the course of commercial activities. This privacy policy applies to personal information of students, parents/guardians, alumni, employees, and volunteers of the school.

Definitions

Personal information is the recorded information about an identifiable individual in any format, including but not limited to:

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation and marital or family status of the individual;
- (b) information relating to the education, medical, psychiatric, psychological, criminal or employment history of the individual, including job performance, or information relating to financial transactions in which the individual has been involved, including income and claims;
- (c) any identifying number, symbol or other particular assigned to the individual;
- (d) the address, telephone number, fingerprints or blood type of the individual;
- (e) the personal opinions or views of the individual except if they relate to another individual;
- (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

- (g) information about physical appearance, lifestyle, leisure activities, academic records, relationships, marital history, immigration status, travel or movement detail, legal proceedings, career history, insurance policy and claims;
- (h) the views or opinions of another individual about the individual; and
- (i) the individual's name as it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Informed Consent requires the person consenting to understand the nature of the information for which consent is sought, understand the potential consequences of signing the consent form, and be given the right to revoke the consent at any time.

Before disclosing a record, the School shall provide notice to any person to whom the information in the record relates if it is practical to do so:

- (a) written notice to the applicant to respond to a *Municipal Freedom of Information and Protection of Privacy Act* request for information;
- (b) written notice to the applicant and to any person to whom the information in the record relates to the decision to disclosure or refusal to disclose, including appeal procedures; and;
- (c) written notice regarding the legal authority for the collection, the principal purpose or purposes for which the personal information is intended to be used, and a contact individual who can answer questions regarding the collection.

Retention time is the minimum amount of time to keep a record as determined to be necessary by law or other authority. Original records cannot be destroyed until the retention time has expired. Likewise, records should not be retained longer than the retention time without good reason.

Disclosure means to make the information available or release it to another institution or person but does not include using the information.

Access means the authority or permission to consult records or to obtain restricted information.

Security means the protection of personal information, regardless of the format in which it is held, and includes, but is not limited to, physical measures such as locked filing cabinets and restricted offices, organizational measures such as limited access, and technological measures such as the use of passwords and encryption.

Collection means to gather, acquire, receive, or obtain the information by means from any source.

Policy

John Knox Christian School values its relationship with its students, parents and guardians, alumni, employees and volunteers and is committed to the protection of their personal information.

Accountability

The School is responsible for personal information in its custody and under its control. The Principal of the School has been appointed as the Chief Privacy Officer assigned to oversee the implementation of this policy. The Principal may designate various individuals with responsibilities relative to maintaining and storing personal information.

The duties of the Chief Privacy Officer include:

- overseeing the development of, and on a regular basis, reviewing The School policies and practices related to privacy to ensure consistent implementation and compliance;
- ensuring staff are trained on privacy best practices and are aware of the importance of safeguarding any personal information that they are privy to;
- ensuring that all inquiries and complaints relating to privacy are appropriately handled;
- ensuring all third parties to whom The School provides access to personal information adhere to appropriate standards of care in managing that information; and
- informing the Board about significant privacy breaches that could potentially cause harm to The School or its reputation.

As noted above, The School may hire service providers to perform services on its behalf. The School provides them with a limited amount of information which is necessary in order for them to provide the services required. They are prohibited from using the information for purposes other than to facilitate and carry out the services they have been engaged to provide and are not permitted to disclose this information to others. The School will strive to protect personal information disclosed to third parties by contractual agreements requiring that those third parties adhere to confidentiality and security procedures and protections, similar to those outlined in the Safeguards section of this document.

In some cases, personal information that the school manages may be transferred, processed and stored outside Canada, and therefore may be available to government authorities under lawful orders and laws applicable therein.

Identifying Purposes

The School will identify and document the purposes for which it collects, uses, or discloses personal information at or before the time of collection. The purposes will be limited to those that are related to the School's business and activities, such as:

- to process applications and open and maintain a student file;
- to exchange personal information with the Ontario Ministry of Education in order to assign, update and validate the Ontario Education Number and the personal information associated with them
- to maintain a record of a student's course of study, evaluations, academic and other achievements;
- to communicate with students and parents about matters related to the student's attendance, evaluation, course of study, and School activities and events;
- to maintain contact with and notify alumni of activities, events, services, and other matters relating to the School;
- in connection with fundraising initiatives;
- for billing and processing of fees and donations;
- to communicate with designated contacts about and to manage emergencies;
- to obtain insurance and file insurance claims;
- in connection with a sale or other transaction or reorganization of the School's operations;
- to comply with legal requirements and co-operate with law enforcement activities.
- to recruit, process applications, evaluate an applicant's suitability for employment or volunteer position, including review of Criminal Records, hire/retain individuals and monitor vacancies;
- to establish, maintain, and terminate records of the employment/volunteer relationship;
- to administer payroll, expenses, benefits, and provide services;
- to comply with statutory requirements including those related to taxation;
- to communicate or publicize information about School business, events and services;
- to monitor and appraise performance;
- to provide development and training activities;
- to monitor time, attendance and leaves of absence;
- to administer health and safety requirements;
- to apply for grants, and in connection with other funding opportunities;
- to comply with applicable employment and human rights legislation;
- to communicate with the individual's designated contact in an emergency;
- to comply with legal requirements and cooperate with law enforcement activities;
- to complete administrative requirements related to The School, to comply with governance requirements or legislation

Consent

The School only collects, uses, or discloses personal information with the knowledge and consent of the individual to whom it relates (or their parent or guardian), except where otherwise permitted or required by law. Consent may be obtained in person, by mail or via the Internet.

The School will not, as a condition of employment or volunteering, require an employee or volunteer to consent to the collection, use, or disclosure of personal information beyond that which is required for those purposes.

In determining whether implied or explicit consent is required and, if so, which form of consent is appropriate, The School will take into account the sensitivity of the personal information at issue, the purposes for which The School will use the information and any legal requirements. Consent may be implied based upon the reasonable expectations of the individual. For example, if you provide personal information in response to a fundraising communication, consent may be implied for the purposes of using the information for fundraising. In determining the appropriate form of consent, The School will take into account the sensitivity of the personal information. Implied consent will generally be appropriate where the personal information is non-sensitive in nature and context.

Limiting Collection

The School will collect, use and disclose personal information for the purposes identified above, for purposes identified outside of this Policy, or where otherwise permitted or required by law.

Limiting Use, Disclosure and Retention

The School will not use or disclose personal information for purposes other than those for which it was collected, except with consent or as permitted or required by law.

The School retains personal information for as long as required to fulfill the identified purposes or to comply with statutory retention periods.

Personal information that has been used by the School to make a decision about a potential employee, an employee or volunteer will be retained for at least one year after the decision has been made.

The School destroys or makes anonymous personal information that it no longer needs for the identified purposes or legal requirements.

Accuracy

The School will use its best efforts to ensure that personal information is as accurate and complete as is necessary for the purposes for which the information is to be used. The School asks students, parents, and alumni to update personal information they have provided to the School as it changes. It asks employees and volunteers to correct out-dated personal information, such as residential addresses and other contact information.

If an employee or volunteer demonstrates to the School that their personal information is inaccurate or incomplete, the School will correct or complete the Personal Information. Requests for correction should be made to the Chief Privacy Officer.

Safeguards

To protect personal information against loss, theft, and unauthorized access, disclosure, use, and modification, the technical safeguards will be monitored by our IT Service provider:

Administrative Safeguards	Technical Safeguards to Protect Electronic Data	Physical Safeguards
<ul style="list-style-type: none"> • privacy and security policies and procedures 	<ul style="list-style-type: none"> • strong authentication and access controls 	<ul style="list-style-type: none"> • controlled access to locations where personal information is stored
<ul style="list-style-type: none"> • privacy and security training 	<ul style="list-style-type: none"> • logging, auditing and monitoring 	<ul style="list-style-type: none"> • locked cabinets
<ul style="list-style-type: none"> • confidentiality agreements for all individuals with access to privacy information 	<ul style="list-style-type: none"> • strong passwords and encryption 	<ul style="list-style-type: none"> • locked doors/access keys limited
<ul style="list-style-type: none"> • privacy impact assessments 	<ul style="list-style-type: none"> • maintaining up to date software by applying the latest security patches 	<ul style="list-style-type: none"> • identification, screening and supervision of visitors
<ul style="list-style-type: none"> • security clearances and permitting access on a “need to know” basis only 	<ul style="list-style-type: none"> • firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, and or anti spyware software 	<ul style="list-style-type: none"> • locking up of personal information and not leaving in plain view or unattended
	<ul style="list-style-type: none"> • protection against malicious and mobile code 	<ul style="list-style-type: none"> •
	<ul style="list-style-type: none"> • threat risk assessments 	<ul style="list-style-type: none"> •

Openness

Through this Policy, the School makes available a general account of its personal information management practices, including the purposes for which it uses and discloses personal information, instructions on how to gain access to and correct personal information and how to obtain additional information about the School's privacy practices and/or its use and disclosure of particular personal information.

Access, Correction, Inquiries

Upon written request, and proper validation of identity, the School will provide an individual with information about its use and disclosure of personal information (and, if applicable, their child's personal information), and except in limited circumstances, will give the individual access to personal information.

Except in limited circumstances, including where doing so would reveal personal information about another individual; the student, employee, or volunteer will be permitted to review their own personal information in the presence of a designated employee of the School.

The School will correct or complete personal information, on the written request of an individual, where it is satisfied the information is inaccurate or incomplete.

Individuals are invited to direct any requests for access or correction and any questions they may have about this Policy, the School's privacy practices, or the School's management of their personal information to the Chief Privacy Officer (or designate) whose contact information is provided below.

The School will respond to written requests for correction or access as promptly as possible. The School may ask for additional information it needs to process a request and/or to verify identity and ensure that it does not disclose personal information to someone who is not authorized to receive it or otherwise in violation of this Policy.

Compliance

The School requires compliance by its employees with this Policy, enforces that requirement, and exercises care in the disposal of personal information to prevent unauthorized access. Any School individual is invited to bring any concerns or questions concerning the School's compliance with this Policy or personal information management to the Chief Privacy Officer (the principal) or designate.

Chief Privacy Officer:

George Petrusma (Principal)
gpetrusma@jkcs-oakville.ca
905-829-8048

Approved by the JKCS Board on **May 28th, 2024**