Eunoia Forest School
Privacy Policy

Created: April 11, 2021
Effective: April 11, 2021
Modified: July 30, 2021
Modified: August 14, 2021
Revised: March 27, 2022

Note: *Owner/Operator* refers to the Owner/Operator or Designate

Contents

Purpose

We enact this Privacy Policy to:

- safeguard the privacy of your personal information
- respect your privacy rights
- uphold our responsibilities under *Personal Information Protection and Electronic Documents Act (PIPEDA)* and *Canada's Anti-Spam Legislation (CASL)* and
- ensure you are aware of:
    - our practices related to your personal information and
    - how we will address any privacy concerns you may have.

Policy

- We follow *PIPEDA*'s fair information principles:

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

- We collect, use, and disclose personal information only for the purposes that a reasonable person would consider appropriate in the circumstances.
    - We limit the collection of personal information (the amount and the type) to what is necessary for identified purposes.
    - We do not:
        - collect personal information indiscriminately,
        - collect, use, or disclose personal information in ways that are unlawful or likely to cause harm,
        - profile or categorize individuals in any manner that leads to unfair, unethical, or discriminatory treatment contrary to human rights law, or
        - publish personal information unless you have provided consent.
- We protect all personal information that we receive, including any personal information transferred to third parties for the purposes detailed under Disclosure.
- Recognizing that privacy breaches could expose you to significant harm, we make conscientious efforts to reduce the risks of unauthorized access, modification, or disclosure of your personal information.
    - We review this Privacy Policy and our practices annually in February and whenever significant changes occur to ensure that our practices are current and effective.
        - Such reviews include an assessment of risks, including new and residual risks and acceptable levels of risk.
        - Significant changes that may instigate a review and that are considered when conducting a review include changes in:
            - our organization,
            - technology,
            - our business objectives and processes,
            - the threat environment, and
            - external events, including changes to the legal or regulatory environment, contractual obligations, and the contexts in which risks arose.
    - We endeavour to detect, contain, report, investigate, and correct any incidents or complaints that arise in a timely and consistent manner.

    - We use external parties compliant with the Payment Card Industry Data Security Standards to process credit and debit card transactions: NMI and Paysafe through CampMinder.
- We uphold your right to:
    - access any personal information that we hold about you,
    - challenge the accuracy and completeness of such information, and
    - have such information amended, as appropriate.

For easier reading, we use the terms *staff* and *employee* throughout this document to refer to paid and volunteer roles at Eunoia Forest School (Eunoia).

Procedures

Collection

- We collect your IP address when you visit our website and/or register for a program online.
- We collect your email address when you sign up to be notified of events, fundraisers, or other service updates and promotional information.
    - We may collect information about what links you click when you open our emails.
- We collect the following information when you apply to register for a program:
    - your full name and relation to your child,
    - name, birth date or age, and grade of your child,
    - if relevant and if you decide, the name of an additional parent/guardian(s) and their relation to your child,
    - your email address,
    - your child's home address,
    - your phone number,
    - your registration requests and preferences,
    - emergency contact information for your child,
    - how you will pay for enrollment,
    - a photo of your child,
    - whether your child has medical conditions or needs, special needs (including for diet, rest, and/or exercise) and/or requires accommodations,
    - information as to whether your child has any restrictions on activity,
    - information as to whether anyone is not authorized to pick up your child,
    - any other information you choose to disclose that you feel may be important for Eunoia staff to know to support your child's experience at Eunoia, and
    - how you heard about us.
- In addition, we collect the following information to complete your registration:
    - additional home address(es), as relevant,

    - telephone number(s) and, if applicable, the name and address of a business/school at which you and any additional parent/guardian(s) can be reached in the event of an emergency during program,
    - name and phone number of an addition emergency contacts if only 1 has been provided,
    - names and phone numbers of any adults who you authorize to pick up your child at the end of program,
    - your child's history of communicable disease and conditions requiring medical attention,
    - any symptoms indicative of ill health,
    - instructions for any medication or medical treatment that must be administered to your child during program and/or regarding any special diet, rest, or physical requirements (e.g., activity restrictions) of your child,
      and
    - information related to the care of your child (e.g., administration of insect repellent, sunscreen, lipbalm, lotion, and/or hand sanitizer).
- Where applicable, we may also collect, in writing, verbally, through observation, or via other means:
    - information about your child's allergies, health, or medical history relevant to their well-being while participating in our programs,
        - We indicate what information is mandatory to provide in related forms and policies.
    - family information relevant to ensuring that your child is in safe care after leaving the program (e.g., custody agreements),
    - responses to COVID-19 screening questions or COVID-19 screening results,
    - the dates and times you entered and exited our program spaces (e.g., while we are following COVID-19 or outbreak protocols),
    - formal complaints and documentation of our resolution process,
    - information pertaining to medication administration, behaviour, accommodations, individualized needs, incidents, unusual occurrences, your concerns, and/or our concerns, as outlined in Eunoia's policies and procedures,
    - additional information you choose to disclose that you feel may be important for Eunoia staff to know to support your child's experience at Eunoia,
      and/or
    - information about a dual relationship with you disclosed by a staff member or volunteer.
- With your permission, we may also collect:
    - photographs and other pedagogical documentation of your child's participation in our programs
      and/or
    - your credit and/or debit card information.
- We also keep a record of your transactions and outstanding debts.
- We date your personal information when it is collected, updated, or verified.
- Please update your information as it changes, especially:

    - contact information,
    - allergy, medical, and health information,
    - names and phone numbers of emergency contacts,
    - custody information,
      and
    - information about people authorized to pick up your child.
        - The Owner/Operator will contact you before the start of your first summer program in a given year to review your registration information. We will update our records accordingly.
            - You will be asked to respond with an email or to complete an electronic form to update your information or verify that your information is accurate, complete, and timely.
- We ask you to sign and date the personal information that you provide and we sign and date any notes in your file as a testament to the accuracy of the information.

Use

- We collect personal information to:
    - communicate with you (e.g., discuss your child's learning and well-being, update you about what your child is doing throughout their time in the program, inform you of your status on a waiting list, etc.),
    - verify that our programs can meet your child's learning and development needs,
    - ensure that children leave our programs only with safe adults,
    - verify that you reside within Ontario as per our insurance requirements,
    - improve our services and respond to any issues or concerns you may have,
    - promote the health, well-being, learning, and development of your child and all children and staff in our programs, including as we plan curriculum,
    - trace contacts, as necessary,
    - notify you about events, fundraisers, or other service updates and promotional information, unless you withdraw consent for these communications,
      and
    - carry out administrative functions (e.g., monitoring statistics and filing taxes).
- As permitted, we use photographs and other pedagogical documentation of your child's participation in our programs to:
    - update you about what your child is doing and learning throughout their time in the program
      and
    - demonstrate and promote Eunoia's activities on our website and in other print and electronic media.
- If you input your card information, we use your credit and/or debit card information to accept payment.
- As necessary, we use your personal information for anti-fraud purposes.

- We use GoDaddy Website + Marketing Analytics and cookies on our website, which allows us to track your IP address, time of visit, header information and location, but no other personally identifiable information. GoDaddy controls how the tracked data is collected and processed, and GoDaddy and its wholly owned subsidiaries may retain and use the tracked information, subject to the terms of its privacy policy.
- We seek consent before using personal information for any purpose other than the purpose for which it was collected.

Consent

- We obtain meaningful consent for the collection, use, and disclosure of personal information.
    - We do not accept any personal information requiring your express consent before you read, understand, and consent to this Privacy Policy.
        - If a third party will be providing your personal information, they must show the Owner/Operator documentation indicating that you have read, understand, and agree to Eunoia's Privacy Policy and that you consent to the third party disclosing your personal information.
- We will ask for your consent again whenever we make a significant change to our privacy policy (e.g., when we add a new use for your personal information or plan to share your personal information with a new third party)
    - We may ask for your consent via prompts on our website or by sending you a consent form via email or, if requested, on paper.
        - We may look at what links you have clicked in our communications to verify that you have clicked the link consenting to continue receiving communications.
- In most cases, consent will be obtained electronically or in writing. If consent is obtained orally (e.g., to break down language barriers), we will record when and to whom you gave consent.
- Our records indicate:
    - all identified purposes for your personal information
      and
    - any consents you have given.
- While we encourage families to provide information that will facilitate the delivery of safe, high-quality individualized services that support their child's learning, development, and well-being, providing personal information is not mandatory to participate in Eunoia's programs.
- You may withdraw your consent at any time, subject to reasonable notice and legal requirements.
    - We will act upon your withdrawal (including unsubscribe requests) as quickly as possible and within 10 business days, at no cost to you.
- We will remind you of the consent choices that you have made and your consent options each time that you register for one or more programs.

- In addition to consent from parents/guardians, we will support children's rights by seeking their assent or consent for collecting and sharing photo(s), video(s), audio recordings, and/or other representations of the child and/or their creations. We also consider children's preferences for sharing information when developing Individualized Plans (IPs) with families. We will not collect photo(s), video(s), audio recordings, and/or other representations of the child and/or their creations if the parent/guardian denies consent (even if the child assents or consents) or if the child denies assent or consent (even if the parent/guardian consents).
- When you enroll in, or inquire about, our programs, you have implied consent to receive commercial electronic messages from us (e.g., notifications about upcoming events).
- When sending electronic messages for marketing and other purposes, we will always include:
    - an opt-out link or button,
    - a reminder of the consent choices you have made and your consent options,
    - our business name,
      and
    - accurate business contact information that will be valid for at least 60 days after you send the message, including: a current mailing address and either a phone number, email or website address.
- We periodically audit our communications with you to ensure they align with current personal information management practices.

Disclosure

- We seek written consent before disclosing personal information for any purpose other than the purposes for which it was collected or any purpose outlined below.

Disclosure Within Eunoia

- The Owner/Operator will access any of the personal information that we collect, only as necessary.
- Employees access only the personal information they need to facilitate safe, individualized learning experiences or to perform their administrative roles, and only after they have read, understood, and agreed to this Privacy Policy.
    - IPs and ISPs are shared within Eunoia according to the consent provided by a parent/guardian or the staff member or volunteer who is the subject of the IP.
- The Owner/Operator and Administrative Assistant are the only Eunoia staff members who will access your credit and/or debit card information.

Disclosure Beyond Eunoia

- Eunoia will share information about your child's participation in a program (e.g., incident reports, pedagogical documentation, and attendance) with all of your child's parents/guardians unless you provide a court order advising against such disclosure.

    - Personal information about you or your child's other parent(s)/guardian(s) will not be shared when information about your child's participation is shared.
- Your personal information is transferred to GoDaddy and processed by GoDaddy, Microsoft, and their respective affiliates, subsidiaries, and service providers when you visit our website (in the case of an IP address), complete a registration form, email us, or subscribe to our newsletter online. GoDaddy and Microsoft will not use or permit its sub-processors to use your personal information beyond the purposes we have intended, beyond the purposes we have agreed to in the Microsoft Customer Agreement/Microsoft 365 Terms of Use and GoDaddy's Universal Terms of Service Agreement, or beyond what is required by law.
- Personal information collected about or in relation to registered students is processed by CampMinder, LLC, which:
    - uses cookies and similar technologies and may use the information collected through these technologies for their own purposes,
    - uses third party service providers, which have their own terms of use and privacy policies and may use cookies and similar technologies to collect information for their own purposes, to deliver its products and services,
    - may collect location data, with your consent,
    - may share your personal information with their service providers, subprocessors, and any of their current or future affiliated entities, subsidiaries, and parent companies,
    - may use your personal information for its own purposes,
    - may make information in photos and videos available to others, subject to your rights and choices,
    - may process your personal information for purposes determined to be in the public interest or as otherwise permitted or required by law,
      and
    - processes and handles your personal information as described in its Terms of Service and Privacy Policy.
- Your personal information may be disclosed to Durham Region Public Health as required (e.g., to facilitate contact tracing or an outbreak response).
- Your name and address are inputted into QuickBooks, which we use to track payments and prepare and send invoices. This means your personal information is:
    - shared with Intuit Inc.,
    - may be transferred to third parties used by Intuit Inc. to deliver its services/products,
      and
    - is used and/or disclosed in accordance with the Intuit Privacy Statement and Intuit Terms of Service for QuickBooks Online, QuickBooks Online Accountant, QuickBooks Self Employed, Payroll Services, QuickBooks Time and QuickBooks Online Accountant Pro Tax Services for QuickBooks Online CANADA.
- Your name, contact information, and transactions may be shared with a third party accounting service and/or may be disclosed to the Canada Revenue Agency as part of tax filing or a tax audit.

    - We will first ensure that the accounting service reads, understands, and agrees to follow this Privacy Policy.
- If you consent, photographs and other pedagogical documentation of your child's learning may be transmitted to the Remind app (Remind101, Inc.).
    - This means:
        - information such as your name and photos, videos, and/or audio of your child may be visible to other people in Eunoia, including families whose children attend program during the same week as your child,
        - your personal information will be transferred to, and processed in, the United States,
        - your personal information may be shared with companies providing service to Remind,
        - your personal contact information will be shared with Eunoia's administrators,
        - your User Submissions (e.g., personal information and messaging) may be visible to Eunoia's administrators if you associate your account with Eunoia,
        - Remind may use your information for its own purposes (e.g., internal operations),
        - identifiers from your device or computer and statistics about your usage of the app may be shared with a third party by Remind,
        and
        - information about you and your child shared through Remind is otherwise subject to Remind's Privacy Policy.
- If you have consented that photographs and other pedagogical documentation of your child's learning may be used for demonstration and promotional purposes, your personal information may be shared with potential funders, lenders, partners, and members of the general public or may be used by GoDaddy.
- If you choose to pay by credit or debit card, your name and payment card information will be transferred to CampMinder, which processes payments using NMI and Paysafe.
    - You input your own payment information, unless you need assistance from the Owner/Operator or Administrative Assistant. The payment information you input in CampMinder is used only as necessary to process the transactions you request.
- If you choose to communicate with us via the contact form on our website and if you email eunoiascreening@gmail.com, your personal information is provided to Google, which may use your information for its own purposes according to its Privacy Policy and Terms of Service.
- If you choose to communicate with us via Instagram or Facebook or share content on our Instagram and/or Facebook pages, your personal information may be used by Meta Platforms, Inc., and/or other companies, and/or members of the public for their own purposes, as described in the Data Policy for Instagram/Facebook/Meta.

- Your personal information will be disclosed to the appropriate Children's Aid Society (CAS) if we suspect child abuse and CAS requires your personal information for their investigation or next steps.
- Anonymized data regarding program attendance may be shared with potential funders, lenders, and partners.
- When transferred or submitted to third parties, your personal information is sometimes sent outside of Canada (e.g., information submitted to CampMinder and information exchanged over our website and email is processed outside of Canada), where it may be accessible to courts, law enforcement, and national security authorities in that jurisdiction.
- Your personal information will otherwise only be disclosed:
    - as required by law (e.g., to courts in response to a warrant or court order, to an ombudsman, to authorities vested in provincial or federal statutes, to a Coroner's Office, to the Minister of Education and officials to whom he/she has delegated authority),
    - if disclosing the information is clearly in an individual's best interests (e.g., to medical personnel in an emergency) and consent cannot be obtained in a timely manner,
      and/or
    - where necessary and permitted by *PIPEDA* for security and investigative purposes.
        - We document when information is disclosed in such circumstances, including a clear rationale for our decision to disclose your personal information.
- When transferring personal information to third parties, we will:
    - Ensure, through contractual or other means, that the third party provides protection comparable to what is required in *PIPEDA*
    - Limit the third party's use of your personal information to the purposes specified to fulfill the contract or seek your consent to transfer your personal information
- Your personal information is not shared over public networks.
- We only transmit personal information when necessary and after ensuring that the transmission is clearly addressed only to the intended recipient.
- When accessing personal information, we position ourselves to ensure that the information is not visible to others who do not have the need or right to see the information.
- Any disclosure requests from third parties are directed to, and managed by, the Privacy Officer.

Storage

Retention Periods

- We retain your personal information only for as long as it is needed for its intended use(s).
- Each COVID-19 screening log and record of who entered Eunoia is retained for 30 days or 1 month (whichever is longer).
- Attendance records are maintained for 30 days or 1 month (whichever is longer).
- Outbreak Line Listing Forms, and Routine Illness Surveillance Forms are maintained for 30 days or 1 month (whichever is longer) from the date of the last entry in the record.
- We retain your email address for at least 30 days (in the case of contact information collected for possible COVID tracing), or as long as your child is enrolled in a program or you are a subscriber to our newsletter (whichever is longer).
- Documentation regarding dual relationships is retained for 99 years.
- Incident reports and any documentation regarding any reports of and/or responses to child abuse are kept for 99 years.
    - Otherwise, your child's file (e.g., registration information, pedagogical documentation, notes about any individualized service planning, complaint discussions, or other personal information used to make a decision about your child) is retained until the March after your child turns 25 years.
        - Thus, your IP address may be retained until the March after your child turns 25 years.
- Credit and/or debit card information is retained in CampMinder for as long as you ask CampMinder to retain such information.
- Records of transactions and outstanding debts are retained for at least, for 6 years from the end of the calendar year in which the transaction was processed. Otherwise, such information is retained for as long as your family is enrolled at Eunoia or for 6 years from the end of the calendar year in which the debt was paid off, whichever is longer.
        - We will retain your personal information for longer than the specified timeframes if the information is the subject of a personal information request or complaint or if otherwise required by law (e.g., to complete an investigation). In such circumstances, we will retain your personal information for as long as is necessary to allow you to exhaust any recourse under PIPEDA and/or for the minimum amount of time necessary.
    - Photographs and other pedagogical documentation of your child's participation in our programs collected for marketing purposes with your consent, may be retained for as long as Eunoia is an entity.
- We maintain an inventory of what personal information is retained, for what purpose, for how long, and where (including back-up files and copies).
- We conduct a review of personal information (to determine what information is no longer needed) and access controls (to verify that each staff member only has access to the personal information required for their duties) annually in March.

Protecting the Security of Your Information

- We never make or keep copies of personal identification.
- Physical records are stored in a single locked cabinet in between program sessions and are stored safely out of unauthorized view during programs.
    - The locked cabinet is only accessed by the Owner/Operator or, if the Owner/Operator grants permission, by staff who need access to carry out their duties.
- Personal information is retained on encrypted laptop(s), mobile phone(s), hard drive(s), and/or tablet(s) and in encrypted cloud storage.
    - We store only the personal information that needs to be accessed on any given device, particularly mobile devices. Personal information is removed from mobile devices as soon as the information is no longer needed, within the parameters of our data retention timelines (e.g., ensuring personal information that must be retained and is not needed on a mobile device is retained elsewhere before removing).
- Whenever possible (e.g., except when we are offsite and a locked cabinet is unavailable), paper and electronic files and electronic devices are locked when not in use.
    - Automatic lock is enabled on devices used for Eunoia business whenever possible.
    - Automatic time-out and 2-factor authentication is enabled on accounts used for Eunoia business whenever possible.
- Eunoia's tablets are equipped with the capacity to be tracked or erased if lost or stolen.
- Eunoia's mobile devices are only used outside of our administrative office or program spaces under the approval of the Owner/Operator.
- We maintain an up-to-date inventory of Eunoia software and hardware and audit this inventory, including physically checking all storage media containing personal information, annually in February.
    - The Owner/Operator or Administrative Assistant maintains a record of when, where, and to whom mobile devices are assigned for use outside of the administrative office.
        - Mobile devices are only used by staff members who have authority to access the personal information on the device.
        - The Owner/Operator or Administrative Assistant also maintains a record of whether devices have been returned.
    - Any inventory discrepancies are investigated and addressed by the Privacy Officer.
- We follow these password practices on all devices and accounts used for Eunoia business:
    - We set and manage strong passwords.
        - A strong password is:
            - unique to the device or account
            - 8 or more characters

            - not an obvious choice that someone may be able to guess and
            - changed at least every 6 months.
    - Passwords are not visible or known to anyone except the single account user.
    - We do not use a password manager.
    - We disable automatic sign-in and “remember password” functions.
- Staff members only access Eunoia files and accounts via secured devices and networks approved by the Owner/Operator.
    - All staff members using personal devices for Eunoia business are accountable for protecting the security and privacy of personal information in their custody, including when configuring the device, modifying or changing device settings, connecting to wireless networks, or installing, updating, or uninstalling apps or software. Employees will patch and update operating systems or complete other security-related updates as prompted by their devices, software, and apps in a prompt manner.
- Eunoia’s wireless network(s) are secured, and their security is monitored, tested, and updated monthly.
    - Only devices authorized by the Owner/Operator may connect to Eunoia’s network.
    - Up-to-date internet security and firewall software are installed and maintained on devices accessing the wireless network and are configured to automatically perform anti-malware definition updates, real-time scans of malicious software, and periodic full system scans.
    - Reports generated by anti-virus software regarding activities on the wireless network are reviewed monthly.
- Anti-virus and firewall software/programs are installed on all Eunoia- or employee-owned devices used to access your personal information.
    - We promptly enable updates as prompted by the software/programs or by a review of our risks and practices.
- Each staff member reduces the risk of spam threatening your personal information through these email practices:
        - enabling a spam filter,
        - not clicking on suspicious links and, preferably, pasting URLs into browsers instead of clicking links,
        - using email that uses a HTTPS connection and encrypts all messages
        - never responding to suspicious emails or text messages, and
        - carefully assessing emails with attachments, even when the emails come from known sources.
- Staff do not use Eunoia-owned mobile devices for personal purposes.
- Employees will not add any apps or software to Eunoia-owned devices without approval from the Owner/Operator.
- We restrict installed apps from accessing your personal information, unless you have consented to such access.

- The Owner/Operator or Administrative Assistant assigns each staff member a unique log-in (identifier) before they may access cloud storage or databases/accounts with personal information.
    - The Owner/Operator or Administrative Assistant manages each user's permissions, limiting access to that necessary for each staff member to carry out their job-related duties.
    - The Owner/Operator or Administrative Assistant keeps a record of the identifier and permissions assigned to each employee.
- We monitor our cloud storage for unauthorized access, including through monthly audits.
    - We maintain a current inventory of any staff-owned devices and email accounts used for work purposes in order to monitor and restrict access to the Eunoia cloud storage.
- Staff members will not share a device or account holding your personal information with anyone outside of Eunoia or with any staff member who does not have authority to access the personal information held within the device or account.
- If a staff member changes a personal device they use for Eunoia business, they must notify the Owner/Operator and the disposal procedures below will be followed.
- Employees must immediately report to the Owner/Operator if their device is lost or stolen or if the security of their device is otherwise compromised. The Incident Management procedures will be followed.
- Staff members will provide written, signed verification that all personal information is removed from their devices according to the disposal procedures below when their employment or volunteer hours with Eunoia end.
- Staff of Eunoia will make every effort to protect the security and privacy of your personal information if their personal device is involved in investigations or litigation.
- We check for compliance with this Privacy Policy before adopting any new hardware, software, application, or cloud technology.

Disposal

- We safely dispose of personal information when it is no longer needed for its intended use(s) or required by law.
- At the time of disposal, all associated copies and back-up files are discarded.
- We irreversibly destroy, erase, or anonymize any personal information that is no longer needed via methods that protect against privacy breaches.
- All electronic media to be discarded or reused will be brought to the Privacy Officer, who will arrange for the appropriate method of data destruction.
- If we decide to recycle electronic devices, we will follow the Environmental Protection Agency's (EPA) recommendations.
- As recommended by the Office of the Privacy Commissioner of Canada (OPC), we follow the National Institute of Standard and Technology's (NIST) guidelines for media sanitization, choosing stronger methods of destruction whenever practical and especially when the media is leaving Eunoia:

Media	Disposal Method
Paper	Cross-cut shredder that produces particles no larger than 1 mm x 5 mm
Router	Follow the manufacturer's instructions for clearing or purging
iPhone/iPad	1. Encrypt any removable storage 2. Remove the removable storage 3. Navigate the device's settings to select full sanitization with Cryptographic Erase supported (encryption on) 4. Manually navigate to browser history, files, photos, and other areas of the device to verify that no personal information has been retained
Printer	Refer to the manufacturer's instructions to purge, then complete the steps recommended by NIST. If purging is not possible, pulverize or incinerate at a licensed incinerator.
Hard Disk Drive	Use the appropriate method for the type of hard drive
Other	Consult the NIST document

- We will test any software or hardware chosen for disposal before relying upon it.
- If we lack the tools to appropriately destroy data or if the volume of data to be destroyed is great, we may contract a third party to safely destroy the data. First, we will ensure that:
    - the contractor has verifiable credentials and can guarantee both a secure transfer of records from our administrative office to their own destruction facility and a secure destruction method that matches the media and information sensitivity,
    - the third party and any possible subcontractors provide the same level of protection under the law as we do, as guaranteed in privacy protection clauses within our contract with the third party,
    - the contractor has a satisfactory track record and conducts periodic audits,

and
    - the contractor reads, understands, and agrees to follow this Privacy Policy.

Accessing and Correcting Your Personal Information

Making a Request

- To request access to, or a correction to, the personal information that we hold about you, you must contact the Privacy Officer at ellisha@eunoiaforestschool.ca with the following information:
    - your email address or your name,
    - your child's name,
      and
    - the date of your registration request or registration, if applicable
- Your request must be made in writing.
- If you need help to make a request, we will assist you.
- Whenever requested, staff will provide the name, address, and phone number of Eunoia's Privacy Officer.

When We Receive Your Request

- We will record the date we receive your request.
- We will review your request and contact you if we need clarification.

Responding to Your Request

- We will provide your personal information as quickly as possible and within 30 days.
    - If meeting this timeline would unreasonably interfere with Eunoia's activities or if we need additional time to conduct consultations or convert your personal information into an alternate format, we will advise you within 30 days of receiving your request and notify you of your right to complain to the OPC. We will provide your personal information within an additional 30 days or according to the time required for converting the information into an alternate format.
- We will provide your information on a cost-recovery basis. We will notify you of the cost and confirm your desire to proceed before fulfilling your request.
- We will identify all sources and records that may hold the personal information that you are requesting and confirm that the sources/records contain the information.
    - We will conduct thorough searches of electronic and physical records and notify you if we have no personal information to disclose.
- We will photocopy and number any paper documents, making sure the copies are clear and readable.
    - If a large number of documents are involved, we may invite you to our administrative office to review the documents.

- We will provide your personal information in alternate format(s) if conversion is reasonable and necessary for you to exercise your rights under *PIPEDA*.
- If requested, we will explain how your personal information is or has been used. We will provide a list of any organizations to which your personal information has been disclosed; if this is not possible, we will provide a list of any organizations to which your personal information may have been disclosed.
- We will ensure that the information we provide is understandable.
    - We will explain acronyms, abbreviations, and codes.
- If you show that the personal information we have is inaccurate or incomplete, we will amend the information and send on the correct information to any third parties to whom we have disclosed the information. If we do not agree that the information was inaccurate or incomplete, we will retain a record of the unresolved challenge and, when appropriate, transmit this record to any third party to whom we may have disclosed the original information.
- We protect the personal information of third parties when responding to requests for access to personal information.
- If some personal information cannot be provided, we will provide as much information as we can within the exceptions permitted under *PIPEDA* (e.g., by severing a file or blacking out text). We will inform you if there is information that we cannot provide.
- We will keep a copy of files as they were sent to you.
- We will only disclose personal information if we are certain of your identity and right of access.
- The Privacy Officer approves all decisions related to your request.
- You can contact Ellisha Blair at ellisha@eunoiaforestschool.ca (416-453-3895/105 Consumers Drive, Unit 2, Whitby, ON L1N 3C4) if you have any questions.

When we Will Not Disclose Your Personal Information

- We may deny your request if:
    - disclosure would reveal personal information about someone else that cannot be severed, blacked out, stricken, or removed, unless the third party consents to the release of their personal information or somebody's life, health, or security is threatened,
    - disclosure of the information could reasonably be expected to threaten the life or security of another individual and the information cannot be severed, and/or
    - we have disclosed your personal information to an investigative body and that body has indicated that your information may not be shared.
- If we refuse to grant your request, we will inform you in writing and explain why.
    - If you are dissatisfied, we will discuss the matter further with you and try to reach a resolution.
    - You also have a right to file a complaint with the OPC about our refusal or any other issues related to your request.

- If we refuse to share your personal information under the direction of an investigative body, we will immediately notify the OPC in writing.

Incident Management (such as a Privacy Breach)

- Employees are responsible for reporting any known, suspected, or potential privacy breaches to the Privacy Officer immediately upon discovery.
- If the employee is able to immediately contain the breach, they will do so. Otherwise, the Privacy Officer will take steps to immediately contain the breach, such as:
    - stopping the unauthorized practice,
    - recovering breached records,
    - shutting down a breached system,
    - revoking or changing device passwords,
      and/or
    - strengthening physical security measures.
- The Privacy Officer will lead an investigation, which will include:
    - determining who needs to be made aware of the incident (while being cautious not to compromise the ability to investigate the breach),
    - analyzing the reasons for the breach,
      and
    - determining and delegating authority to enact steps for mitigating risks associated with the incident (while being cautious not to destroy evidence that may be valuable in determining causes or appropriate corrective actions). A prevention plan may be developed, with consideration for:
        - physical and technical security,
        - policies and procedures,
        - employee training practices,
          and
        - partnerships and contracts with third parties.
- We review our incident management process annually in February.

Notifying You and Reporting the Breach

- If your personal information is accessed, modified, or disclosed in contradiction to this Privacy Policy, either within or outside of Eunoia, we will:
    - notify you, affected individuals, and relevant third parties if the breach constitutes a real risk of significant harm,
    - report the breach to the OPC if it constitutes a real risk of significant harm,
      and
    - keep a record of the breach.
        - We will provide all information outlined by the OPC when providing these notifications or updating our records.

Compliance

- The Owner/Operator, Ellisha Blair, is Eunoia's Privacy Officer responsible for Eunoia's *PIPEDA* compliance.
- In addition to technical standards and the practices in this Privacy Policy, staff are expected to exercise good judgment and reasonable caution to protect the security and confidentiality of your personal information.
    - Staff agree to protect the security and confidentiality of personal information when signing this Privacy Policy upon hiring and annually thereafter.
    - We will provide employees with adequate and ongoing privacy training to ensure they understand and will comply with this Privacy Policy. Training will prepare employees to:
        - respond to inquiries regarding our Privacy Policy in plain language,
        - explain what personal information is collected, why, and how it is used,
        - understand valid and meaningful consent and how and when it is obtained,
        - recognize and respond to requests for personal information,
        - respond to incidents,
        - identify the person to whom privacy-related complaints should be directed,
        - manage their devices and accounts to protect your personal information,
        - respect privacy when sending emails (including when and how to use BCC),
          and
        - understand Eunoia's current or new initiatives for protecting personal information.
- We will conduct an annual privacy impact assessment using the OPC's privacy self-assessment tools in February each year.
    - We will set and achieve prompt timelines for addressing any shortcomings in our privacy practices.

Complaints and Inquiries

- To make a complaint or inquire about our personal information handling, contact our our Privacy Officer:
    - call 416-453-3895,
    - mail 105 Consumers Drive, Unit 2, Whitby, ON L1N 3C4,
      or
    - email ellisha@eunoiaforeschool.ca.
- We will investigate any privacy-related complaints we receive through the following process:

    - We will acknowledge your complaint and seek clarification if needed.
    - We will identify a senior staff member who can review your complaint fairly, impartially, knowledgeably, competently, promptly, and efficiently. We will provide this person with all relevant records and connect them with anyone who handled your personal information or your access request.
    - We will improve any practices and policies that are deemed problematic to the security and privacy of your personal information.
    - We will notify you of our findings clearly and promptly. We will also notify you of any steps we have taken.
    - We will notify our employees of any changes to our policies and procedures.
- We record our responses to complaints to promote consistency.
- You have a right to file a complaint with the OPC at any time. If relevant, you may also seek recourse through a regulatory body (e.g., the College of Early Childhood Educators, the Ontario College of Teachers, or the Ontario College of Social Workers and Social Service Workers).

Glossary

Breach Loss of personal information or unauthorized access to, use of, copying of, modification of, or disclosure of personal information

Electronic files Information stored on electronic media such as hard drives, USB flash drives, and mobile phones

Meaningful consent Consent is valid if a person can reasonably understand the nature, purpose, and consequence of the collection, use, and/or disclosure of their personal information

Mobile devices Includes portable devices and removable media (e.g., laptops, tablets, smartphones, USBs, and external hard drives)

Office of the Privacy Commissioner of Canada (OPC) An agent of Canadian parliament responsible for protecting and promoting privacy rights

Personal information In *PIPEDA* (2019), “any factual or subjective information, recorded or not, about an identifiable individual”

Physical records Hard copies of data, including notes, memos, messages, correspondence, transaction records and reports (e.g., incident reports and Eunoia’s Daily Written Record)

PIPEDA *Personal Information Protection and Electronic Documents Act,* Canada’s law governing how businesses use personal information in the course of commercial activities

Significant harm As described in *PIPEDA* (2019), includes bodily harm, humiliation, damage to reputation or relationships, financial loss, identity theft, negative effects on the credit record, damage to or loss of property, and loss of employment, business, or professional opportunities

We The Owner/Operator and all paid personnel and volunteers of Eunoia Forest School

You The person providing personal information (about themself, their child, or someone else) to Eunoia

Sources

Government of Canada. (2019). *Getting consent to send email*. Retrieved from https://www.fightspam.gc.ca/eic/site/030.nsf/eng/00008.html

Government of Canada. (2019). *Securing your business' computers, devices and networks to prevent spam*. Retrieved from https://www.fightspam.gc.ca/eic/site/030.nsf/eng/00010.html

Government of Canada. (2019). *Using business best practices for spam protection*. Retrieved from https://www.fightspam.gc.ca/eic/site/030.nsf/eng/00011.html

Office of the Information & Privacy Commissioner for British Columbia. (2015). *IT security and employee privacy: Tips and guidance*. Retrieved from https://www.oipc.bc.ca/guidance-documents/1807

Office of the Privacy Commissioner of Canada. (2013). *Ten tips for avoiding complaints to the OPC*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/02_05_d_55_tips/

Office of the Privacy Commissioner of Canada. (2013). *Interpretation bulletin: Personal information*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/

Office of the Privacy Commissioner of Canada. (2014). *Tips for federal institutions using portable storage devices*. Retrieved from

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/privacy-act-compliance-help/02_05_d_58_psd/

Office of the Privacy Commissioner of Canada. (2014). *Frequently asked questions for online consent*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_oc_201405_faq/

Office of the Privacy Commissioner of Canada. (2014). *Personal information retention and disposal: Principles and best practices*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/gd_rd_201406/

Office of the Privacy Commissioner of Canada. (2015). *Is a Bring Your Own Device (BYOD) program the right choice for your organization?* Retrieved from https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/gd_byod_201508/

Office of the Privacy Commissioner of Canada. (2015). *Securing personal information: A self-assessment tool for organizations*. Retrieved from https://services.priv.gc.ca/securite-security/en

Office of the Privacy Commissioner of Canada. (2016). *Electronic and digital payments and privacy*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/02_05_d_68_dp/

Office of the Privacy Commissioner of Canada. (2016). *Protecting personal information on your mobile devices.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/technology/mobile-and-digital-devices/digital-devices/02_05_d_47_dpd/

Office of the Privacy Commissioner of Canada. (2018). *Preventing and responding to a privacy breach*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/c-t_201809_pb/

Office of the Privacy Commissioner of Canada. (2018). *Ten tips for a better online privacy policy and improved privacy practice transparency*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/02_05_d_56_tips2/

Office of the Privacy Commissioner of Canada. (2020). *Privacy guide for businesses*. Retrieved from https://www.priv.gc.ca/media/2038/guide_org_e.pdf