Privacy, Security, and Confidentiality Policy

Date Issued: November 29, 2022	**Last Reviewed:** November 2022
Approved By: S. Karnay	**Seconded By:** S. Shadrin
Applies to: LDANR Personnel, Clients and Stakeholders	

Intent

Protecting the privacy and confidentiality of personal and business information is of the utmost importance to the Learning Disabilities Association of Niagara Region ("LDANR"). Collecting, using, and disclosing personal and business information appropriately, responsibly, ethically, and in accordance with all applicable statutory requirements is fundamental to the LDANR's operations.

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") establishes rules to govern the collection, use, and disclosure of personal information. The LDANR is committed to protecting and respecting the personal information of its clients, staff, volunteers, business partners, and all other entities it interacts with in accordance with the Privacy Act and PIPEDA practices.

The LDANR acknowledges that we must collect potentially sensitive information to properly attend to the individuals involved with our programs and services, which mandates us to diligently manage the collection, use, and disclosure of personal information in a manner that recognizes the right to privacy of individual's personal information.

This policy outlines the LDANR's commitment to privacy, security and confidentiality, and establishes the methods and security measures by which privacy and confidentiality are ensured.

Definitions

All definitions sourced from PIPEDA.

Term	Definition
Breach of Security Safeguards	The loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards, or from a failure to establish those safeguards.
Personal Information	Any factual or subjective identifying information about an individual or group of individuals. This can include name, date of birth, address, income, e-mail address, social insurance number, gender, evaluations, credit records, and so forth.

Business Information	Business information related to a specific business that is not readily available to the public, such as names of executive officers, business registration numbers, proprietary information, and financial status. Business information is treated and handled with the same level of confidentiality, privacy, and respect as personal information. Business Information includes but is not limited to: • Client lists • Client medical information • Client personal information • Labour relations • Human resource planning, policies or procedures • Company financial information, status and statements • Any information, or documentation labelled "Confidential" by the LDANR, or listed as such by separate memorandum, or e-mail that informs of confidential status • Any information pertaining to LDANR's clients, staff, volunteers, and visitors Any information relating to the LDANR that is freely in the public domain may not be considered "Confidential". In the event that an employee can prove that information was possessed before it was received from LDANR, or that information was gained from an unrelated third party, said information will not be classified as "Confidential".
Security Safeguards	Security safeguards include the following but are not limited to: • Physical measures (e.g., locking filing cabinets and restricting access to offices); • Organizational measures (e.g., limiting access on a "need-to-know" basis); • Technological measures (e.g., the use of passwords and encryption).
Significant Harm	Includes bodily harm; humiliation; damage to reputation or relationships; loss of employment, business, or professional opportunities; financial loss; identity theft; negative effects on a credit record; and damage to or loss of property.

Guidelines

It is understood that LDANR personnel will become aware of personal information regarding our clients, staff and/or volunteers, and business information regarding the LDANR through the course of their involvement. The LDANR requires that all personnel, including anyone delivering or involved with services on behalf of LDANR, keep all personal information regarding our clients, staff, and/or volunteers, and all business information regarding the LDANR confidential both during and after their term of involvement.

LDANR personnel must abide by the procedures and practices set out in this policy while handling personal and business information in a confidential and appropriate manner to ensure that our client, staff, volunteer, stakeholder, and business information is safe, and that individuals can feel assured knowing that we are actively working to keep their information secure. LDANR personnel understand that if confidential information is not effectively protected, the operations of LDANR may be threatened, and the well-being and privacy of our clients, staff and volunteers may suffer irreparably.

The LDANR assumes full accountability for the personal information within its possession and control. The Executive Director and Board of Directors are responsible for privacy matters and legal compliance with privacy laws, although all LDANR office staff equally contribute to the implementation and upholding of privacy processes. It will be a collaborative effort amongst all LDANR office staff to ensure:

- The collection, use, retention, destruction, management and protection of personal information is conducted in a confidential manner;
- Complaints and inquiries regarding privacy and confidentiality are investigated and responded to;
- The training of personnel on privacy and confidentiality;
- The use of privacy agreements and contracts to ensure the protection of personal information where the information must be provided to a third party; and
- That policies and procedures pertaining to the following are created, reviewed and revised as appropriate.

I. Collection of Information

In the course of conducting its business, the LDANR will obtain personal information directly from the individual to whom the information belongs, or their caregiver if under the age of majority. To protect the privacy of individuals involved with the LDANR, the LDANR only collects the minimum amount of personal information required to ensure the satisfaction and safety of any individual involved with the LDANR.

The LDANR will abide by the following practices for collecting personal information:

- Individuals must be informed as to why personal information is being collected. Before being asked to provide consent, individuals will be provided with the reasons their personal information is being collected, how it will be used and stored, what options are available to the individual regarding the collection, use, and disclosure of personal information, any disclosure or possible disclosure of the information, and how the individual may access and correct any inaccuracies in their personal information.

Obtaining Consent for Collection of Information

- Consent must be obtained for the collection and use of information. Consent occurs and is considered obtained by the LDANR when an individual, or an individual authorized on their behalf, provides express consent orally, in writing, or through an applicable online action. This occurs each time an individual completes a form or application for the LDANR. The consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose, and consequences of the collection, use, or disclosure of the personal information. Implied consent is granted by the individual where consent may reasonably be inferred from the action or inaction of the individual. Where possible, this should always be followed up by a LDANR representative to obtain express consent.
- The LDANR may use personal information without the individual's consent under particular circumstances. These situations include, but are not limited to:
    - The collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
    - The personal information was produced by the individual in the course of their employment, business, or profession, and the collection is consistent with the purposes for which the information was provided;
    - The collection is made for the purpose of making a disclosure required by law; or
    - Any other reason as defined in applicable legislation.
- Individuals have the right to withdraw their consent, although this may impact their involvement in the LDANR's programs and services. If an individual wishes to limit who is able to access certain portions of their personal information, they may do so by notifying a LDANR office staff in writing.

Accuracy of Personal Information

- All personal information collected is accurate. The LDANR encourages our clients, staff and volunteers, or those authorized to act on their behalf, to contact us with any changes to personal information that may be relevant to our ability to provide timely and effective services. Individuals are allowed access to their personal information, and to make corrections as appropriate. In most instances, the LDANR will grant individuals access to personal information in the care, custody, and control of the company upon

presentation of a written or verbal request and satisfactory identification. If an individual finds errors of fact with their personal information, they should notify the LDANR as soon as possible to make the appropriate corrections or change the information that they have access to. If the LDANR denies an individual's request for access to their personal information, they will advise in writing of the reason for such a refusal. The individual may then challenge the decision.

II. Use of Information

Appropriate Use

The LDANR uses personal information solely for the purpose of conducting business and developing an understanding of individuals involved with the LDANR. The LDANR hereby asserts that personal information may only be used to:

- Ensure the safe and efficient delivery of programs and services;
- Assess eligibility and/or needs;
- Maintain contact about programs and services;
- Prevent harm or respond to emergency situations;
- Plan, administer and manage our internal operations;
- Compile statistics and other reporting requirements as mandated by our funders;
- Contact individuals regarding upcoming LDANR opportunities such as specific events, activities and services that may be of interest.

The LDANR will abide by the following practices for using personal information:

- Personal information is used only for the purposes for which it was collected, except with the consent of the individual or as required by law. Personal information collected is only collected, used, or disclosed for purposes that a reasonable person would consider appropriate in the circumstances. Individuals must be notified and consent must be obtained before using personal information for any reason other than those provided at the time of collection.
- Under no circumstances will the LDANR sell, distribute, or otherwise disclose personal information, including personal contact information or employee lists, to third parties, unless required to do so by law. This may include consultants, suppliers, or business partners of the LDANR, but only with the understanding that these parties obey and abide by this policy, to the extent necessary of fulfilling their own business duties and day-to-day operations.

III. Storage and Protection of Information

The LDANR will abide by the following practices for storing and protecting personal information:

- All personal information in LDANR possession or custody must be protected.
- The LDANR will take every reasonable precaution to protect personal information with appropriate security safeguards and precautions. The LDANR maintains personal information through a combination of paper and electronic files. Paper files are kept in locked cabinets. The electronic information we keep is stored on a secure server as well as in an electronic database.
- The LDANR will retain personal information only for the duration it is needed for conducting its business and ensuring statutory compliance. Once personal information is no longer required, it will be destroyed promptly, safely, and securely. However, certain laws may require that certain personal information be kept for a specified amount of time. Where this is the case, the law will supersede this policy.

IV. Security Safeguards

Physical Measures

- Active physical files are kept in locked filing cabinets.
- Only active LDANR office staff and designated Board members have keys to enter the LDANR offices.
- Only active LDANR office staff and designated Board members have access cards to enter the building.
- The LDANR will keep record of all personnel who have keys and access cards.
- Upon termination, personnel return keys and access cards to the LDANR office.
- Lost keys or access cards are reported to the Executive Director.

Organizational Measures

- Access to personal and confidential business information is authorized only for the LDANR personnel who require the information to perform their job duties, and to those otherwise authorized by law.
- All LDANR personnel are required to sign a Confidentiality Agreement confirming their adherence to this policy and commitment to protect the personal information of clients, staff and volunteers and LDANR business information. Violation of this agreement will result in disciplinary action. Consequences could include termination of the individual's relationship with the agency and/or legal action. This agreement remains in force even after an individual's relationship with the agency has ended.
- All LDANR personnel are trained regarding privacy responsibilities.

Technological Measures

- The LDANR will stay abreast of common security threats utilizing information from various software and/or digital platform providers and will update policies and procedures as needed to ensure information remains secure across devices.
- The LDANR's computer network systems, accounts, and databases are secured by complex and secure passwords and firewalls to which only authorized individuals may access.
- While IP addresses may be logged in order to administer the LDANR website, these IP addresses will not be linked to any personally identifiable information.
- Any digital form asking site visitors to enter personal or financial information will be protected by SSL encryption.
- Automatic alerts are in place to be sent to the Executive Director when a possible security threat occurs.
- A "Notice of Confidentiality" is added to all original outgoing emails.
- Computer software and devices are kept updated for optimal security.
- LDANR account passwords are changed each time an individual with authorized account access leaves LDANR.
- Personnel inform their supervisor when changes to company passwords are made.
- Personnel avoid using the same passwords across accounts.
- Personnel access to files is protected by Multi-Factor Authentication, where possible.
- Routers and servers connected to the Internet are protected by a firewall, and are further protected against virus attacks or "snooping" by sufficient software solutions.
- Digitally stored files are housed in software solutions compliant with privacy legislation.

LDANR personnel must exercise all cybersecurity best security practices when engaging with digital content. These security practices include but are not limited to:

- Use extreme caution when opening e-mail attachments received from unknown senders which may contain viruses.
- Avoid clicking links or downloading content from unknown sources sent in a direct message or otherwise.

LDANR personnel are strictly prohibited from:

- Sharing account passwords with unauthorized employees, customers, or third parties.
- Transferring personal or confidential business information to employees, volunteers, or any other person in the LDANR unless authorized.
- Connecting LDANR social media accounts to other third-party apps unless approved by the Executive Director.
- Leaving devices that are signed into LDANR social media accounts unlocked or unattended.

- Participating in quizzes or challenges on LDANR's social media that ask for personal information.
- Participating in phishing schemes by offering personal or confidential company information.
- Changing established privacy settings unless authorized to do so by the Executive Director.

V. Breaches of Security Safeguards

Reporting Data & Privacy Breaches

If LDANR becomes aware of a breach of our security safeguards that compromises the privacy of the personal information retained by the LDANR, the following action shall be taken:

- If a LDANR personnel detects a breach in security, they must report it to the Executive Director and/or Board of Directors immediately.
- The Executive Director will ensure the Board of Directors are made aware as soon as feasible once it has been determined that a breach has occurred.
- The Executive Director and/or Board of Directors is responsible for coordinating the response to the breach and ensuring that all reasonable action is taken to address the breach.
- The Executive Director, Board of Directors, or an appointed LDANR office staff member, will notify any affected individuals of the breach as soon as feasible.
- LDANR will maintain records of every breach of security safeguards. The record should include the following:
    - A description of the circumstances of the breach and, if known, the cause;
    - The date on which, or the period during 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 extent that the information is known;
    - The number of individuals affected by the breach or, if unknown, the approximate number;
    - A description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;
    - A description of the steps that the organization has taken or intends to take to notify affected individuals of the breach.

Notifying Affected Individuals

The LDANR will first assess the following factors when determining whether a security breach constitutes a real risk of significant harm to an individual or individuals:

- The sensitivity of the personal information involved in the breach;
- The probability that the personal information has been, is being, or will be misused; and
- Any other prescribed factor.

The Executive Director is responsible for ensuring that all individuals for whom the breach creates a real risk of significant harm are notified at the earliest available opportunity, subject to any legal restrictions, in a form of communication that a reasonable person would consider appropriate in the circumstances. Notifications shall contain sufficient information to allow the individual to understand the significance to them of the breach, including:

- A description of the circumstances of the breach;
- The date on which or period during 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 extent 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;
- Contact information that the affected individual can use to obtain further information about the breach; and
- Any other prescribed information.

The notice shall be conspicuous and given directly or indirectly to the individual in the prescribed form and manner as legislatively required as the situation dictates.

In addition to the individuals affected by the breach, the LDANR may notify other parties of the breach or disclose personal information relating to the breach, subject to the following guidelines:

- LDANR will notify other organizations, government institutions, or parts of government institutions if LDANR believes that doing so can reduce or mitigate the harm from the breach.
- LDANR may disclose personal information without the knowledge or consent of the individual if:
    - The disclosure is made to the other organization, the government institution, or the part of a government institution that was notified under the breach; and

- The disclosure is made solely for the purpose of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.

VI. Complaints or Concerns

Any questions or concerns regarding the use of personal information can be directed to info@LDANiagara.org or (905) 641-1021. The LDANR will investigate and respond to concerns to the best of its abilities about any aspect of the handling of personal information.

VII. Nondisclosure

In working for the LDANR, personnel shall not divulge, disclose, provide or disseminate confidential business information to any third party not involved with the LDANR at any time, unless the LDANR Executive Director or Board Chair gives written authorization. Furthermore, confidential business information shall not be used for any purpose other than its reasonable use in the normal performance of employment or position duties for the LDANR.

VIII. Legal

This agreement will not supersede any legal obligation to disseminate information when required to do so in a court of law.