

Personal Information Protection and Disclosure Policy of the Legal Information Clinic at McGill

Guiding statement: The LICM commits to only collecting personal information on an as-needed basis, and to restrict the use of this information to the purposes for which it was collected. All information remains confidential, and is disclosed only to those who require it for the provision of services. All non-essential information transmitted by employees, volunteers, credited students, or clients will be immediately destroyed upon reception.

Section 1: Information Collected by the LICM

The types of personal information collected are as follows:

- **Employees:**
 - Information necessary for the hiring, communication with, and remuneration of employees. This includes: legal name, permanent and/or mailing address, telephone number, email address, social insurance number, emergency contact information (telephone), and direct-deposit banking information.
- **Volunteers & Credited Students:**
 - Information necessary for contact and hiring of volunteers and credited students. This includes: legal name, telephone number, email address, year of study, current educational institution, and CV.
- **Clients:**
 - **Legal Information Clients:**
 - First name, telephone number, email address, relationship (if any) to McGill University, and any relevant information disclosed by the client in order to assist them with their legal situation.
 - **Legal Advice Clients:**
 - Full name, preferred name, pronouns and prefix, phone number, occupation, email address, home address, relationship (if any) to McGill University, other involved parties in the client's legal situation and their phone number, and any relevant information and/or documents disclosed by the client in order to assist them with their legal situation
 - **Student Advocacy Clients:**
 - Full name, preferred name, pronouns, phone number, email address, student number, program and year of study, and any relevant information

and/or documents disclosed by the client in order to assist them with their situation

- **Commissioner-for-Oaths Clients:**
 - Personal documentation of a varying nature, as provided by the clients for commissioning. Such documents are only collected and retained by the Clinic where the service is provided virtually.

Section 2: Consent to collection of personal information

The personal information enumerated in Section 1 of this Policy is only collected following the express consent of the concerned individual.

- In the case of employees, volunteers, or credited students, this consent is expressed upon the submission of their application to the position in questions, which shall inform them of their rights under the *Act respecting the protection of personal information in the private sector*
- In the case of legal advice and student advocacy clients, this consent will be obtained upon signature of the client's contract with the LICM.
- In the case of legal information clients, this consent will be expressed upon agreement to create a file with the Clinic, after being informed in accordance with Article 8 of the *Act respecting the protection of personal information in the private sector*.
- In the case of Commissioner-for-Oaths Clients, this consent will be expressed upon a request to create an appointment for the said services, after being informed in accordance with Article 8 of the *Act respecting the protection of personal information in the private sector*.

Section 3: Use, storage, and access to personal information

The personal information of employees and clients are to be used and stored as outlined below:

- **Employees:**
 - Use: the personal information of employees will be used only for the purposes of establishing and maintaining the employment relationship, and to ensure the effective and timely payment of wages
 - Storage: all personal information collected for the aforementioned uses will be stored in digital format in the Executive Director's electronic files, on a cloud-based service, in accordance with the terms of service that may apply for the electronic service provider. Any documents received via email will be transferred to the Executive Director's general file management system, and the relevant records will be promptly removed from the email service.

- Access: access to files containing employees' personal information disclosed for employment purposes is restricted to the Executive Director.
- **Volunteers and Credited Students:**
 - Use: personal contact information of volunteers and credited students will only be used for the purposes of hiring them and communicating with them in the course of their mandates at the Legal Information Clinic at McGill. The personal information of volunteers and credited students might also be used for disciplinary measures.
 - Storage: all personal information collected for the aforementioned uses will be stored in digital format on the directors' shared electronic files.
 - Access: access to volunteers and credited students' personal information will be limited to the current directors of the Legal Information Clinic at McGill, the supervising lawyer, and the current senior caseworkers, as the case may be. Personal information from credited students will be restricted to the current directors of the Legal Information Clinic at McGill only.
- **Legal Information Clients:**
 - Use: personal contact information of legal information clients will only be used for the purposes of developing legal research questions, retrieving the client's file, and for communications with the client. Other personal information relating to a client's legal questions may be used for educational/training, or statistical purposes after ensuring personal/identifying characteristics have been removed.
 - Storage: all personal information collected for the aforementioned uses will be stored in digital format on the IssueTrack software. Client information is never taken outside the clinic, **unless under the supervision of a Director and for case management or research purposes**, and volunteer caseworkers are never entitled to keep this information in personal files.
 - Access: access to clients' personal information will be limited to volunteer caseworkers during their management of the case. Directors-on-duty are responsible for supervising the volunteer's interactions with the client, and such Directors will only access a client's file in order to ensure the proper handling of the case.
- **Legal Advice Clients:**
 - Use: personal information of legal advice clients and/or potential clients will only be used to verify if the mandate can be taken on by the clinic (area of law, legal questions, conflict of interests check), retrieving the client's file, communications with the client, and fulfilling the limited mandate agreed upon with the clients.

- Storage: all personal information collected for the aforementioned uses will be stored in digital format on the software used by the Clinic. Client information is never taken out of the clinic, **unless under the supervision of the lawyer and for case management purposes**, and client files are accessed only on the database with clinic computers.
 - Access: access to the client files is restricted to the Executive Director, the supervising lawyer, and the student advisor assigned to the case. To access the digital database, authorized members of the clinic have to go through a two-factor authentication process.
- **Student Advocacy Clients:**
 - Use: personal information of student advocacy clients will be used to verify if the mandate can be taken on by the clinic (issue, conflict of interest check), retrieving the client's file, communications with the client by the Director, senior advocates or the junior advocate assigned to the client and communications on the client's behalf with members of the McGill community, subject to the client's consent.
 - Storage: all personal information collected for the aforementioned uses will be stored in digital format on Google Workspace. Client information is only accessed by the Director of Student Advocacy, senior advocates and the junior advocate assigned to a client, and can be accessed only with permissions given through Google workspace. Cases of a sensitive nature (subject to Director's discretion) will be subject to an additional password protection on the file
 - Access: Access to client files is restricted to the Executive Director, Director of Student Advocacy, senior advocates and the student advocate assigned to the case. To access the file, permissions must be given by the senior advocate team or the Director of Student Advocacy. Cases of a sensitive nature will have restricted access based on a password protection put in place by the Director of Student Advocacy
- **Commissioner-for-Oaths Clients:**
 - Use: documents received electronically will only be used for the purposes of verifying the Client's identity, and for the affixation of the commissioner's stamp, signature and declaration
 - Storage: all personal information collected for the aforementioned uses will be stored in digital format on the Commissioner-for-Oaths email address, as well as on Commissioner's personal computers when downloaded for the affixation of stamp, signature, and declaration.
 - Access: access to clients' personal information is strictly limited to Commissioners who are administering the oath in question.

Section 4: Conservation and retention of personal information

All personal information collected by the LICM will be retained for a maximum period of six (6) years. Notable exceptions to this policy include:

- Legal advice clients: retention for seven (7) years, in accordance with article 18 of the *Règlement sur la comptabilité et les normes d'exercice professionnel des avocats*
- Student Advocacy Clients: retention for ten (10) years, for files pertaining to sexual violence, in accordance with McGill University's policy on Sexual Violence
- Commissioner-for-oaths clients: retention for seven (7) days following the delivery of the service

Section 5: Destruction & deletion of personal information

When the maximum aforementioned period for the retention of personal information has expired, relevant documents will be destroyed and/or deleted as follows:

- Paper / physical copies of personal information: While the Clinic's current preference is for the maintenance of electronic files (either at inception or via scanning/digitization of physical copies), any existing physical copies will be shredded and disposed of via normal waste disposal services.
- Electronic copies: Electronic files containing personal information will be deleted from both the relevant electronic file management system, and from any 'Deleted Items' folders that may retain the information beyond the initial deletion date. Electronic files received via email for the Commissioner-for-Oaths services will be deleted from the email server (including the 'Deleted Items' folder), and are not stored in any other locations. Files downloaded onto personal computers for purposes of signature/certification will similarly be permanently deleted after the expiry of the relevant period.

Section 6: Designated authority

The designated authority responsible for the administration of the LICM's Personal Information and Protection Policy is the Executive Director of the LICM. The Executive Director has, *ex officio*, the sole authority to access all documents retained by the Clinic, at any time, including those that contain the personal information of employees and Clients. The Executive Director is obligated to only exercise this authority for valid reasons, including the administration of the employment relationship and the management of Client files (if escalated to the Executive Director), as well as the management of requests to access personal information retained by the Clinic.

Section 7: Requesting Access to Personal Information

According to articles 30 and 31 of the *Act Respecting Personal Information in the Private Sector*, all persons with personal information held at the Clinic have the right to access copies of their

personal information retained by the Clinic. However, in order to ensure that information is not disclosed to ineligible third parties, individuals must be identifiable in accordance with articles 27 and 30 of the *Act*, and with provision of government-issued photo identification.

In order to request access to their personal information retained by the Clinic, the person may fill out the *Request for Personal Information Access and/or Rectification Form*, which is received by the Executive Director. Upon receipt of such a request, the Executive Director will direct the Director of Student Advocacy & University Affairs or the Clinic's Supervising Lawyer, as the case may be, to retrieve the relevant file. Upon performing the necessary verifications, the Executive Director may transmit the file to the requesting Client within 30 days of the request, if the client can be adequately identified.

In the event that the Executive Director, in consultation with the Director of Student Advocacy & University Affairs or the Clinic's Supervising Lawyer, as the case may be, determines that the request for access must be denied, the Executive Director will inform the client of this refusal, in writing, in accordance with article 34 of the *Act*. In providing this notice, the Executive Director will provide the client with information pertaining to the recourses available to them.