Office of Student Experience
Student Counselling Centre

PRIVACY POLICY

- Privacy of personal information is an important principle to the Student Counselling Centre. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the services we provide. We also try to be open and transparent as to how we handle personal information. This document describes our privacy policies.

WHAT IS PERSONAL HEALTH INFORMATION?

- Personal health information includes information about an identifiable individual. Personal health information includes information that relates to:
    - The physical or mental health of the individual (including family health history);
    - The provision of health care to the individual (including identifying the individual's health care provider);
- Information that relates to: an individual's personal characteristics (e.g., gender, age, income, home address or phone number, ethnic background, family status); health (e.g., health history, health conditions, health services received by them); or, activities and views (e.g., religion, politics, opinions expressed by an individual, an opinion or evaluation of an individual).
- Personal information is in contrast to business information (e.g., an individual's business address and telephone number). This is not protected by privacy legislation.

WHO WE ARE

- The Student Counselling Centre (SCC) is a department within the Office of Student Experience at the University of Windsor.
- The staff includes registered Clinical Psychologists, registered Social Workers, therapists registered with the College of Registered Psychotherapists of Ontario, Psychology and/or Social Work graduate students, and administrative assistants. Clinicians, in the course of their duties, have access to any personal information we hold. However, graduate students are restricted to information about their personal clients only, and do not have access to all files. We have their commitment to follow appropriate privacy/confidentiality principles.
- Other personnel such as security or computer consultants attend our offices only when staff are present, and are not privy to client information. Maintenance staff does not have access to client information.

WHY WE COLLECT PERSONAL INFORMATION

We collect, use, and disclose personal information in order to serve our clients.

- For our clients, the primary purpose for collecting personal health information is to provide therapy, crisis intervention, or to conduct assessments. For example, we collect information about a client's health, educational, and psychosocial history. This information helps us assess what their counselling needs are, to advise them of their options, and then to provide the treatment or assessment to which they have consented.
- A second primary purpose is to obtain a baseline of health and social information so that we can identify changes that occur over time.

We also collect, use, and disclose personal health information for purposes related to or secondary to our primary purposes. The most common examples of our related and secondary purposes are as follows:

- Related purpose #1: To promote our centre, new services, special events, and opportunities (e.g., a seminar, workshop, or group) that we have available. We will always obtain express consent from the client prior to handling personal health information for this purpose.
- Related purpose #2: To provide services and to obtain payment for services or goods provided (e.g., letters, medical certificates).
- Related purpose #3: To provide statistics to university administration, write annual reports, improve our services, write a research article, etc. Information from our client records is collected in a database for the purpose of collating intake and session information, monitoring progress, and/or enabling us to summarize our services. In no case is a client's name ever included in any reporting or research conducted by us. Rather, information is present as group data.
- Related purpose #4: To comply with external regulators. Our professionals are regulated by various colleges who may inspect our records and interview our staff as part of its regulatory activities in the public interest. The colleges have their own strict confidentiality and privacy obligations.

- It is rare for us to collect personal information without the client's express written consent, but this might occur in an emergency (e.g., the client is unconscious) or where we believe the client would consent if asked and it is impractical to obtain consent (e.g., a family member passing a message on from our client and we have no reason to believe that the message is not genuine).

EXCEPTIONS TO PRIVACY

- We keep information about client contact in order to maintain records in line with requirements set by the Canadian Psychological Association Ethical Standards, The College of Psychologists of Ontario, the Ontario College of Social Workers and Social Service Workers, and The College of Registered Psychotherapists of Ontario. Importantly, these organizations may inspect our records and interview our staff as part of their regulatory activities in the public interest.
- Various government agencies (e.g., *Information and Privacy Commissioner*, *Human Rights Commission*, etc.) also have the authority to review our files and interview our staff as part of their mandates. In these circumstances, we would consult with professionals (e.g., university legal counsel) who will investigate the matter and report back to us. In addition, external regulators have their own strict privacy obligations.
- The cost of some services provided by the Student Counselling Centre to clients may be paid for by third parties and these payers often have your consent or legislative authority to direct us to collect and disclose information in order to demonstrate client entitlement to funding (e.g., Bursaries for Students with Disabilities, request for files).
- If there are reasonable grounds to suspect physical, emotional, or sexual abuse of a child under 16-years of age. Reporting reasonable grounds to suspect physical, emotional, or sexual abuse of a person who is 16 or 17-years old is discretionary (CYFSA).
- If there are reasonable grounds to believe that a member of a regulated health profession was sexually intimate with and/or made sexually suggestive or inappropriate remarks to a client/patient (RHPA).

- If there is a court/judge order to release a client's records, a search and seizure warrant, a coroner's warrant, or an urgent demand for records in conjunction with a missing person.
- If there are reasonable grounds that an elderly person residing in a long-term care home or retirement home is being abused or neglected (LTCA; RHA)
- PHIPA permits, when there are reasonable grounds, a disclosure to eliminate or reduce a significant risk of serious bodily harm to self or others.

OUR COMMITMENT TO PRIVACY

We understand the importance of protecting personal information. For that reason, we have taken the following steps:

- Paper information is either under supervision or secured in a locked or restricted area.
- Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, strong passwords are used on computers.
- Personal health information is only stored on mobile devices if necessary. All personal health information stored on mobile devices is protected by strong encryption.
- We try to avoid taking personal health information home to work. However, when we do so, we transport, use, and store the personal health information securely.
- Paper information is transmitted through sealed, addressed envelopes or boxes by reputable companies.
- Electronic information is either anonymized or encrypted before being transmitted.
- Information is sent by FAX only with the consent of the client, and with the understanding that they, or their representative, will personally collect the FAX (e.g., to obtain consent to release information).
- Staff is trained to collect, use and disclose personal information only as necessary to fulfil their duties and in accordance with our privacy policy.
- We do not post any personal information about our clients on social media sites and our staff members are trained on the appropriate use of social media sites.
- External consultants and agencies with access to personal information must enter into privacy agreements with us.

RETENTION AND DESTRUCTION OF PERSONAL INFORMATION

- We need to retain personal information for some time to ensure that we can answer any questions you might have about the services provided and for our own accountability to external regulatory bodies. However, in order to protect your privacy, we do not want to keep personal information for too long.

- We keep our client files for at least 10 years from the date of the last client interaction or from the date the client turns 18.

- We destroy paper files containing personal information by shredding. We destroy electronic information by deleting it in a manner that cannot be restored. When hardware is discarded, we ensure it is reformatted and/or physically destroyed.

YOU CAN LOOK AT YOUR INFORMATION

- You have the right to see what personal information we hold about you, with only a few exceptions. Often, all you have to do is ask, and an appointment can be scheduled with you. We will need to confirm your identity before providing you with this access. We can help you identify

what records we have about you. We will also try to explain any information you do not understand (e.g., short forms, technical language, etc.). We reserve the right to charge a fee for such requests.

- We may ask you to put your request to view your file in writing. We will respond to your request as soon as possible and generally within 30 days, if at all possible. If we cannot give you access, we will tell you the reason, as best we can, as to why we cannot give you access.
- You have the right to ask for information to be corrected if you believe there is a mistake. This applies to factual information, not to any professional opinions we may have formed. We may ask you to provide documentation that our files are wrong. Where we agree that there is a mistake, we will make the correction. At your request and where it is reasonably possible, we will notify anyone to whom we sent this information (but we may deny your request if it would not reasonably have an effect on the ongoing provision of health care). If we do not agree that we have made a mistake, we will still agree to include in our file a brief statement from you on the point.

IF THERE IS A PRIVACY BREACH

While we will take precautions to avoid any breach of your privacy, if there is a loss, theft or unauthorized access of your personal health information we will notify you.

- Upon learning of a possible or known breach, we will take the following steps:

- We will contain the breach to the best of our ability, including by taking the following steps if applicable
    - Retrieving hard copies of personal health information that have been disclosed.
    - Ensuring no copies have been made
    - Taking steps to prevent unauthorized access to electronic information (e.g., change passwords, restrict access, temporarily shut down system)
- We will notify affected individuals
    - We will provide our contact information in case the individual has further questions
    - We will provide the Commissioner's contact information and advise the affected individual of their right to complain to the Commissioner
- We will investigate and remediate the problem, by:
    - Conducting an internal investigation
    - Determining what steps should be taken to prevent future breaches (e.g. changes to policies, additional safeguards)
    - Ensuring staff is appropriately trained and conduct further training if required

Depending on the circumstances of the breach, we may notify and work with the Information and Privacy Commissioner of Ontario. If we take disciplinary action against one of our practitioners [or revoke or restrict the privileges or affiliation of one of our practitioners] for a privacy breach, we are required to report that to the practitioner's regulatory College. We may also report the breach to the relevant regulatory College

DO YOU HAVE A QUESTION OR CONCERN?

- Our Information Officer, Dr. Mohsan Beg, Clinical Director of Student Health and Wellness, will attempt to answer any questions or concerns you might have, and can be reached at:

University of Windsor
Student Counselling Centre
Room 293, 2nd Fl., CAWSC

401 Sunset Ave.
Windsor, Ontario N9B 3P4
(519) 253-3000, Ext. 4616

- If you wish to make a formal complaint about our privacy practices, you may make it in writing to our Information Officer who will acknowledge receipt of your complaint, ensure that it is investigated promptly and that you are provided with a formal written decision with reasons.
- If you have a concern about the professionalism or competence of our services or the mental or physical capacity of any of our professional staff, we would ask you to discuss those concerns with us.
- However, if we cannot satisfy your concerns you are entitled to contact our regulatory body:

The College of Psychologists of Ontario
110 Eglinton Ave. E., Suite 500
Toronto, Ontario M4R 1A3
(416) 961-8817

Ontario College of Social Workers and Social Service Workers
250 Bloor Street East, Suite 1000
Toronto, Ontario M4W 1E6
(416) 972-9882

College of Registered Psychotherapists of Ontario
375 University Avenue, Suite 803
Toronto, Ontario M5G 2J5
(416) 479-4330

- This policy is made under the Personal Health Information Protection Act (2004). This is a complex Act and provides some additional exceptions to the privacy principles that are too detailed to set out here. There are some rare exceptions to the commitments set out above.
- For more general inquiries, the Information and Privacy Commissioner of Ontario oversees the administration of the privacy legislation. The Commissioner also acts as a kind of ombudsman for privacy disputes and can be reached at:

The Information and Privacy Commissioner/Ontario
2 Bloor St East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: Toronto Area (416/local 905): (416) 326-3333
Long Distance: 1 (800) 387-0073 (within Ontario)
TDD/TTY: (416) 325-7539
FAX: (416) 325-9195
www.ipc.on.ca

Policy updated June, 2021.