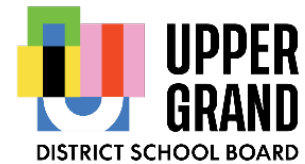


# Privacy Protocol for Child Youth Workers, Social Workers, Psychologists, Psychological Associates and Speech Language Pathologists P.08



## A. SAFEGUARDING STUDENT PERSONAL INFORMATION

1. In order to safeguard personal information required for your work (wherever that work may be done), the following is required:
  - a) unlocked file cabinets will be supervised at all times and locked when unsupervised
  - b) access to paper files and file cabinets will be through designated department staff
  - c) all electronic devices will be password protected
  - d) all electronic devices will be locked when unattended to ensure personal information is not visible on the screen
  - e) all electronic devices will be physically secured when left unattended
  - f) personal information stored on UGCloud will be secured by appropriate sharing settings.
  - g) all personal information stored on electronic devices will be encrypted
2. In order to safeguard personal information on electronic devices while in transit, the following is required:
  - a) electronic devices (e.g., laptops, chromebooks, tablets, smartphones, thumb drives, etc.) are the responsibility of the individual at all times
  - b) electronic devices must be locked away out of sight while unattended (e.g., trunk of car)

---

## **B. TRANSFER OF ELECTRONIC INFORMATION**

### **1. E-mail**

Personal information will not be transferred out of board by e-mail.

### **2. Fax**

Personal information may be transferred by fax when accompanied by a cover sheet containing the “confidentiality warning” and one of the following safeguards:

- a) the fax number has been confirmed by the recipient
- b) the recipient has advised that the fax machine is securely located and there is no basis to doubt the assurance
- c) in the context that the privacy of the recipient of the fax can reasonably be inferred (e.g., it is to an organization that is expected to keep information private like a legal, accounting, or health care agency)
- d) the recipient has a Privacy Policy/Protocol
- e) your incoming fax machine is securely located

### **3. Flash Drive**

Personal information on a flash drive may be transferred in a sealed envelope, clearly marked private and confidential, when:

- a) sent by Canada Post, a reputable courier, or through the Upper Grand District School Board (UGDSB) courier service
- b) delivered in person by staff
- c) picked up by a person who asks for it by the name of the recipient (files must be kept secure until picked up)

## **C. TRANSFER OF PAPER INFORMATION**

Hard copies of personal information may be transferred in a sealed envelope, clearly marked private and confidential, when:

- a) sent by Canada Post, a reputable courier, or through the UGDSB courier service
- b) delivered in person by staff
- c) picked up by a person who asks for it by the name of the recipient (files must be kept secure until picked up)

#### **D. GENERAL SAFEGUARDS**

Staff (including temporary workers) will be trained in the following:

- a) the importance of the privacy of personal information
- b) access to personal information on a need-to-know basis
- c) the UGDSB's Privacy Protocol and how to contact the board's Freedom of Information Coordinator
- d) sensitivity in collecting or using personal information verbally where others might overhear
- e) the removal or masking of unnecessary personal information when providing copies of personal information
- f) the ability to recognize and avoid being pumped for information
- g) that all personal information on paper is to be discarded by shredding
- h) to avoid discussing personal information in public places (e.g., elevators, washrooms, restaurants, etc.)
- i) the need to change passwords on a regular basis
- j) the need to inform individuals if their personal information is misused or misappropriated
- k) reviewing of departmental files for quality assurance while maintaining standards of confidentiality

---

## **E. RETENTION AND DESTRUCTION OF PERSONAL INFORMATION**

- a) Files (electronic and paper) will be maintained in the appropriate Student Support and Program Services file in accordance with the board's Records Management Manual and [Policy 316](#).
- b) Paper files will be destroyed by shredding after completing a Records Destruction Notice which is forwarded to the Records Management Officer for approval, and to follow the proper procedure.
- c) Electronic records will be deleted and electronic storage devices will be destroyed.

## **F. ACCESS, CORRECTION, COMPLAINTS, AND OPENNESS**

### **1. Access Rights**

- a) Access to files by the parent, guardian or students 16 years of age or older will be granted within 30 days, following appropriate College guidelines and unless a ground for refusal exists.
- b) If a refusal exists, the grounds for the refusal will be made clear to the individual requesting the information and any recourse that is available.
- c) Access to information includes personal information held and how it has been used and disclosed (reasonable records must be kept of any unusual uses or disclosure of personal information such as systematic filing of cover letters, fax sheets or e-mails).
- d) If staff are unable to answer a request for access to files, they will refer that request to the supervisor for their department.
- e) If the supervisor is unable to respond to the request for access to the files, the request will be forwarded to the board's Freedom of Information Coordinator.
- f) Test scores may be provided but test forms will not be provided to ensure that the integrity of test protocols is maintained.

- g) Reasonable steps will be taken (and recorded) to ensure that the individual making the request can understand the information (e.g., short forms or codes must be explained, an alternative format is used where the requester has a sensory disability, or an interpreter is used when necessary for English as a Second Language or hearing impaired individuals).

## 2. **Correction requests**

- a) An individual may request that personal information be corrected.
- b) The individual will provide a written request stating the information to be corrected and the reason for seeking the correction.
- c) If the writer of the information agrees to make the change:
  - i) a record of the reason for making the change will be recorded in the file
  - ii) the change will be made in writing
  - iii) the original and the corrected document will both be kept in the file
  - iv) the individual will be informed that they may request that the corrected document be forwarded to any person or organization to whom the individual's record was disclosed within one year prior
- d) If the writer of the information does not agree to make the change:
  - i) the writer will provide a written statement of disagreement to the individual;
  - ii) the individual will be notified in writing that the written request for a correction and the statement of disagreement will be attached to the original document
  - iii) the individual will be informed that they may request that the written request for a correction and the statement of disagreement be forwarded to any person or organization to

whom the individual=s record was disclosed within one year prior

iv) the individual will be informed in writing of the complaints process

### 3. **Complaints Process**

When an individual feels that their issue has not been resolved to their satisfaction by the Student Support and Program Services member,

- a) the individual will be provided with the name and contact information for the board=s Freedom of Information Coordinator
- b) the board=s Freedom of Information Coordinator will investigate the complaint and provide a decision in writing to the individual
  - i) if the individual is not satisfied with the decision, written information will be provided directing them to the office of the Information and Privacy Commissioner of Ontario

### 4. **Breach of Confidentiality**

When a breach of confidentiality occurs:

- a) the Student Support and Program Services member will inform their supervisor
- b) the supervisor will inform the person(s) whose personal information has been breached
- c) the supervisor will inform the Director of Education, the Superintendent of Program, and the Freedom of Information Coordinator
- d) the Freedom of Information Coordinator will inform the Information and Privacy Commissioner of Ontario
- e) the supervisor will meet with the Student Support and Program Services member(s) to review what occurred and how it could have been prevented
- f) the supervisor will review the Privacy Protocol with all staff

- g) changes will be made to the Privacy Protocol to prevent a reoccurrence, if necessary

5. **Openness**

- a) Staff will be trained to provide the Privacy Statement to anyone who requests it.
- b) The Privacy Statement will be posted on the board=s website as an appendix to the Privacy Protocol (See Appendix A).
- c) The Privacy Statement will be given to each parent or guardian of a student referred for services.