Privacy of Information

Part 1

In Ontario, public organizations are subject to the following laws with respect to the privacy of personal information:

- ***Freedom of Information and Protection of Privacy Act (FIPPA)***
- ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)***
- ***Personal Health Information Protection Act (PHIPA)***
- *Part X of the* ***Child, Youth and Family Services Act*** (*CYFSA)*

”Personal information” means recorded information about you as an individual. It may include your name, address, sex, age, education, and medical or employment history. It can also include identifying numbers such as a Social Insurance Number, and your personal views or opinions. Information that may seem personal, such as name and contact information, may not be your personal information if that information relates to your business activities, that is, you are acting in a professional capacity in the context of the information.

Ontario public institutions must protect your personal information in their possession. You have the right to expect that your personal information will only be collected for legitimate, limited and specific purposes, that the collection of your personal information will be limited to only what is necessary for the specified purpose and that your personal information will only be used and disclosed for specified purposes.

An Ontario public institution must tell you:

- under what legal authority they collect your personal information
- how it intends to use the information it collects
- who can answer any questions you may have about how your personal information will be used

In most circumstances, you have the right to see your personal information. If there is an error, you have the right to ask for a correction. There is a process to request your personal information and a process to seek a correction.

If you believe your personal information has been improperly used, you can file a complaint with the organization that has your information. If you do not receive a satisfactory result, you can file a complaint with the office of the Information and Privacy Commissioner using their online form. For more information, go to: Complaints - IPC

The Information and Privacy Commissioner of Ontario (IPC) can help you resolve the problem with the institution or service provider. If, after reviewing the complaint, the IPC decides to process a complaint and then establishes that the organization did not comply with Ontario’s access and privacy laws, we can make recommendations to the institution to prevent it from happening again.

With limited exceptions, the IPC does not have the power, under Ontario’s provincial and municipal privacy laws, to make an order against an institution

related to a privacy complaint. It cannot issue fines, award damages or require that an institution discipline its staff members.

When investigating a complaint under Ontario's child, youth and family services law, and health privacy law, the IPC has the power to issue orders, or "decisions." IPC decisions are binding and require organizations to take certain actions to comply with the law.

This information was sourced from: Your privacy rights - IPC

Resources:

Ontario's Freedom of Information and Protection of Privacy Act, A Mini Guide
provincial guide-e.pdf (ipc.on.ca)

Your Privacy, Ontario's Information and Privacy Commissioner
Your_Privacy-e.pdf (ipc.on.ca)

Part 2

Graham F. Scott wrote an article called, Student Privacy and You, that was published in Professionally Speaking, the magazine of the Ontario College of Teachers. The article included these excerpts:

Seven virtues of privacy protection

The Information and Privacy Commissioner of Ontario and the Access and Privacy Office of the Ontario government offer advice for safeguarding personal information. Here are some steps to take to ensure compliance with MFIPPA.

1. Collect only as much personal information as you need to do your job.
2. Collect information directly from individuals, or for students under 18, directly from their parents or guardians – not from third parties.
3. Explain why you need to collect the information and exactly how it will be used.
4. Get consent from students, or for students under 18, from parents, for the collection, storage and use of personal information.
5. Store personal information securely. Keep hard copies under lock and key, such as in a locked filing cabinet; keep electronic documents on a password-protected computer. A clean desk will help prevent sensitive information being misplaced or stolen.
6. When in doubt, ask for advice from the school principal or the board staff member in charge of privacy. (Ontario law requires every board to have one such contact person.)
7. When you no longer need the personal information to do your job, destroy it by shredding paper documents or securely erasing electronic ones.

The OSR

The Ontario Student Record (OSR) is a good place to start when considering how student information is to be treated. Each student's OSR includes an office index card giving her or his name, student number, address, phone number, gender, birthdate, any enrolment and transfer dates, names of parents and guardians or both, and emergency contact numbers. The OSR also includes report cards and an official student transcript. Some of this information may be duplicated elsewhere or be available to teachers in another form, but the OSR itself – and all the information in it – is to be kept strictly confidential by school boards.

Information from OSRs may be released only under certain circumstances. Students themselves, at any age, have the right to access their records, as do their parents.

Teachers and school officials also have fairly broad – but not universal – leeway to access OSRs. They are allowed to access a student's OSR only for purposes of improving the student's instruction. That broad term, "improvement of instruction," taken from the *Education Act*, means there are many occasions when it's perfectly appropriate to access OSRs. But it's not always appropriate.

Sometimes, with the best of intentions, a teacher can make a mistake. Shanahan offers an example: Teacher-candidates returned from classroom placements and mentioned that one teacher, as a learning opportunity, was planning to hand out a bunch of OSRs so the teacher candidates could get a sense of what they actually contain. "And these are real live OSRs," she recalls. She told the candidates, "That teacher can't do that. You guys [the teacher-candidates]

have no business looking at that stuff, and even teachers have no business looking at it, except for the purpose of educating their students."

Other limited disclosures of information from the OSR are sometimes permitted, such as complying with a court order under the federal criminal code, in a civil suit, or under a court order under the *Child and Family Services Act*.

But even in these cases, principals are advised by the Ministry of Education to consult with their boards' legal counsel before turning over any records. (Teachers are still required to disclose suspicion of abuse to the Children's Aid Society under the *Child and Family Services Act*.)

Use judgment

The best rule of thumb is this: consider whether disclosing information will contribute to improved instruction for the student. Privacy regulations can't make that decision for you. This is where the law steps back and professional ethics take centre stage – in judging just when information-sharing will improve the education of a student, and when it won't. Professional ethical standards provide guidance.

For instance, say that Fatima's parents are divorcing and her marks are slipping as a result. Sharing that information in the staff room with a colleague, so that Fatima can get some extra help and support, will improve her education. Sharing the same information with the same colleague, but this time in the produce aisle at the grocery store, is unlikely to meet professional standards.

"Confidential information about students' lives should not be the source of gossip or frivolous discussion," says Elizabeth Campbell, an associate professor who has taught professional ethics at OISE/UT. "It should be shared sparingly and only when compelled by law, or in cases of helping students and serving their best interests."

To access the complete article, go to: Student Privacy and You - Professionally Speaking - March 2008 (oct.ca)