**Background:**

In 1987 the Ontario Government passed the Freedom of Information and Protection of Privacy Act (FIPPA). FIPPA came into effect for Ontario community colleges on January 1, 1989. The purpose of the legislation was two-fold; to give access to information held by the provincial government and its ministries, agencies and commissions, and at the same time, to protect the privacy of individuals. The privacy of individuals is given additional protection by the stipulation that when information is collected, the reason for its collection shall be given and the information only be used for that purpose, with very limited exceptions.

Sir Sandford Fleming College (Fleming College) is strongly committed to protecting the privacy of our current students and staff, past students and staff and prospective students in accordance with our legal obligations under the FIPPA Act. This legislation specifies how Fleming College must handle (collect, use, disclose, retain) personal information in its custody or under its control, such as student and employee data.

**Purpose:**

The general purpose of this document is to inform Fleming College staff of the type of personal information we may collect about students and staff, under which authority as well as how we may use, disclose and maintain that information. This document is not intended as a replacement but as a support for the college’s obligation to comply with the FIPPA privacy legislation.

**Responsibility for Administration:**

All academic and administrative departments are responsible for the adhering to these procedures governing privacy protection and the act with regard to access to records. Individual college departments are responsible for developing and implementing their own guidelines and procedures to ensure that they reflect the intent of this document and FIPPA legislation. Employees of the college who have access to personal information are accountable for adhering to the responsibilities under this document and the legislation. In addition the College will ensure that reasonable measures are in place to prevent any unauthorized access to all personal information under its control.

Fleming College employees have a responsibility to understand what constitutes personal information, and when working with personal information to collect, use and disclose it only where necessary to perform their individual job duties as per this document. Staff also have the responsibility to control, store and maintain it in a secure manner as to prevent unauthorized disclosure.

The college’s FOI Coordinator is responsible for providing advice to all departments on interpretation of, and on compliance with this document.

**Personal Information: A definition**

Personal information is recorded information about an identifiable individual (who is mentally competent, age 16 and over) including:

* the address, phone number, fingerprints, blood type on an individual
* information relating to the age, race, gender, ethnic origin, sexual orientation, marital/family status of the individual
* information relating to the medical, criminal, employment history or financial transactions/status, educational status, educational history, student’s grades and records and pictures/photos
* Social Insurance Number (SIN), employee number/student number (EMPL ID) or other identifiable number associated with an individual.
* the views or opinions of another individual about an individual (eg.performance or other evaluation comments)
* correspondence sent to the institution by the individual that is implicitly or explicitly of a private or confidential nature and replies to that correspondence
* the individual’s name where it appears with other personal information or where the disclosure of the name would reveal other personal information about the individual.

**Privacy Protection: All faculty, administrative and support staff and students**

Personal information contained in College records will be collected, retained and disclosed in such a way as to protect the privacy of the individual to whom the information pertains. All faculty, administrative and support staff should be aware of the necessity to protect the privacy of individuals and should exercise the utmost discretion when asked for personal information by third parties either in person, in writing, by email, by telephone or other method.

Student personal information:

The basic guideline governing the release of information is as per the FIPPA act and the belief that the college has a responsibility to protect student’s personal information. The college will not release student’s personal information to third parties without the written consent of the student. This applies typically to requests from parents, field placement employers, prospective employers, credit bureaus, banks and other educational institutions. Students may access their own files at the Admissions and Records office; photo identification is required. There are some exceptions to this in the FIPPA legislation and they are noted below.

Staff personal information:

College department offices or individual employees, although they may have access as part of their role within the institution, may not provide any personal information about individuals employed by the College, unless for the purpose for which it was collected, or authorized by the individuals concerned. Personal information, is information about an identifiable employee that is collected and used in the course of employment excluding an employee’s name, position name or title, work address, office location, work telephone number, work email address and work product/role.

Specific guidance on the correct handling of confidential employment records and employee’s personal information can be provided by the Human and Organizational Development Department administration. Relevant sections in the faculty and support staff collective agreements will supersede FIPPA and this document.

**Collection of Personal Information:**

The college will collect or compile and record only personal information as is necessary for the proper administration of the college and its academic programs and ancillary services. The purpose for the collection of personal information shall be made clear to the individual about whom information is requested or compiled, normally by means of a disclaimer or notice of collection on the form. The form or notice will include the following:

* The legal authority for collecting the information (Eg., Ministry of Colleges and Universities Act, Canada Revenue Agency, Collective Agreements, Ministry of Health)
* The authorized principle purpose or purposes for which the information is intended to be used
* A college representative/department who can be contacted to respond to questions about the collection

The personal information must be collected directly from the individual it pertains to, with some limited exceptions including the following:

* Where the individual authorizes another manner of collection
* For the purpose of determining suitability for an award to recognize outstanding achievement
* For the purpose of conducting a proceeding or a possible proceeding before a court or tribunal or for law enforcement

**Use and Disclosure of Personal Information:**

Personal information in our custody or under our control shall only be used according to our obligations under FIPPA as described:

* When the person to whom the information relates has consented to its use
* For the purpose for which it was explicitly collected or compiled or related purposes the individual would have reasonably expected at the time they provided their personal information
* For fundraising activities if the personal information is reasonably necessary for the fundraising activities (subject to certain parameters included in June 2006 amendments to the Act)
* When required to meet our duty to provide a harassment-free and safe college environment, personal information will be shared and used on a ‘need to know’ and case by case basis. Specific use and disclosure decisions will be made by the Care Team within the FIPPA personal information guidelines
* In accordance with the “disclosure of personal information” section below

Personal information in our custody or under our control will not be disclosed in most cases, however some exceptions may apply, including (but not limited to):

* In accordance with an official and approved Freedom of Information request
* Where the person to whom the information related has consented to its disclosure
* For the purpose of complying with an act of federal or provincial legislation, or as required by law
* An officer or employee of the College who needs the record in the performance of his or her legitimate duties or to support activities required for the legally authorized administration of the College.
* An appropriate person in an emergency or for compassionate reasons affecting the health or well-being of an individual or the college community providing the individual is duly notified that such use was made of personal information
* For fundraising activities (subject to certain parameters included in June 2006 amendments to the Act, if the personal information is reasonably necessary for the fundraising activities and provided that College enters an written agreement with the receiving party which meets certain requirements)

Individuals have the right to request correction to their own personal information if they believe an error or omission exists. In most cases individuals have a right of access to any personal information about themselves contained in our custody. However, some exceptions may apply, including (but not limited to):

* Where the disclosure would create an unjustified invasion of another individual’s privacy
* Where the information is supplied in confidence and is evaluative or opinion material complied solely for the purpose of assessing the teaching materials, research, suitability for an honour or award

In the circumstances that the change request is made formally under FIPPA, it will be forwarded immediately to the College’s FOI Coordinator for review and advice. These requests are reported annually to the Ontario Privacy Commissioner.

**Maintenance, Security and Destruction of Personal Records**

Fleming College is committed to ensuring the security of personal information. Records containing personal information relating to faculty, administrative and support staff, retired employees, students, alumni or volunteers which is collected and maintained in a College administrative office or data bank, will be stored in a secure manner. Hard copy files and records are preferably to be kept in lock filing cabinets within offices which are lockable outside of working hours. This document is supplemented by various rules and guidelines adopted in specific academic and administrative departments.

Appropriate security precautions will be taken to safeguard personal information which is stored electronically. To prevent unauthorized access or disclosure, maintain data accuracy, and ensure the appropriate use of information, the college has put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we make accessible online. The Fleming College Information Technology Appropriate Use Policy describes employees’ obligations when using the college’s technology to access personal information.

Personal records shall be retained for a minimum of one year and only be kept as long as they might reasonably be expected to be needed, or as long as required under relevant legislation, collective agreements, contracts or statutes of limitation for the courts. When personal records are no longer required, they will be shredded to protect privacy.

**Other Privacy Legislation**

Personal Health Information Protection Act (PHIPA): This Act applies to health care providers. The College Health Services and College Counselling departments are all required to follow this legislation.

Personal Information Protection and Electronic Documents Act (PIPEDA): This Act applies to all private sector organizations that conduct any commercial activity. The College is not governed by this legislation.

For more information contact the Freedom of Information Coordinator in the Human & Organizational Development Department.

*Appendix A*

*Example collection/purpose of use disclaimers for student personal information:*

*In accordance with section 39(2) of the Freedom of Information and Protection of Privacy Act, any personal information and identifiers, including photographs, will be used for academic/administrative purposes, lists with e-mail addresses/student information databases, submission of assignments to anti-plagiarism software, and photographs will be used for class identification, examinations, promotion committee meetings and campus security requirements.  Your personal information will also be shared with the Sutherland Student Administrative Council or the Frost Student Association, for their administrative purposes to provide support and services for students.*

*Example collection/purpose of use disclaimers for employee personal information:*

*The personal information on this form is collected under the authority of the Ministry of College and Universities Act R.S.O. 1990, cM.19, s.5. In accordance with the Freedom of Information and Protection of Privacy Act, it will be used only for the purpose of administering your payroll and other legally authorized administrative purposes within the college. If you have questions regarding the collection/use/retention of this information, please contact the Payroll department at Sir Sandford Fleming College.*

|  |
| --- |
| *Appendix B: Personal Information - Use and Release Guidelines* |
| Purpose: This guideline has been developed to serve as a model for use of personal information within the college and a guide for release of personal information external to the college.  |
| Principle: The use of personal information within the college as well as release and disclosure to external parties, is based on the Freedom of Information and Protection of Privacy Act. Fleming College is committed to the protection of our student's privacy and guidelines have been developed within our obligations under this act, as well as in consideration of the safety, security and general wellbeing of our student and staff population. |
| Sample Scenario | Information requested and parties involved | Guideline |
|   |   | Internal use | External release |   |
| A Parent has asked if their son or daughter has been going to class as they are concerned that they have not been truthful about their attendance at school | One student's attendance data |   | Parent of Student | Mentally competent individuals aged 16 and older exercise their own access and privacy rights under FIPPA. We will not provide a student's class attendance information without written permission from the student |
| A Parent has asked if their son/daughter has been approved for an OSAP loan | One student's financial data |   | Parent of Student | We will not provide a student's financial information without written permission and would suggest the parent obtain this information from their child. |
| A parent has requested a copy of their son/daughter's timetable to find them at the College. | Student's timetable and program |   | Parent of Student | A Student's timetable is personal information and we would not provide this to any one other the individual student. If this is an emergency, we can suggest that we get a message to the student for the parent . |
| Police officer has requested access to a students program, timetable, as part of an ongoing police investigation | Student's timetable and program |   | Police | Upon proof of the investigation and police badge number, the information will be released. |
| The local newspaper has requested access to information regarding a students current enrolment status at the college, in response to a police investigation | Students enrollment status, program |   | Media | The college will not release this information without written permission from the student |
| Student has logged a harassment complaint concern regarding another student at the college. They do not have the name and the only identification method would be through program area and photos. A request from college administration has been made to the Registrars office to release an array of photos from a particular program area. There is also a request for the student to view the array. | Multiple student photos, names, program | Administrative staff | Students | Administrative staff may have access to the information for security purposes without additional notification as this use is advised at the time of the photo taken.We will not disclose a student's photos to other students. |
| A parent has contacted the school concerned about recent behavior exhibited by their child and has requested counseling information be released to them | Student's mental and medical condition |   | Student's Family  | The college will not release this information unless a serious health or safety concern exists. We could suggest that they discuss with their son/daughter to see if they would give permission for the parents to talk to the counselors, likely with the student present. |
| A college counselor has reasonable grounds to suspect that a student is at risk of committing suicide and this information should immediately be acted on to prevent this. | Student's mental and medical condition | Director of Counseling and internal staff on the care team with a need to know. | Student's Family, Friends and/or Doctor |  College administration will take necessary steps to ensure that the danger is appropriately mitigated, including the contact of relatives and friends. Whenever possible we strive to gain the permission of the client before releasing any personal information relating to them.Decisions are made on a case by case basis.  |
| A parent calls to request personal information regarding their son/daughter and indicates that they are still living at home. Will we change our policy in this case? | Student's personal information |   | Student's Family  | Mentally competent individuals aged 16 and older exercise their own access and privacy rights under FIPPA. Therefore, though they may be minors for other purposes, parents can generally not have access to the personal information of individuals who have reached the age of 16. Place of residence will not alter these access rights. |
| A student requests a 'blanket' release form for their parents to have access to all their personal information at the college.  | Student's personal information |   | Student's Family  | The College requires authorization to be specific, explicit and in a written format. A ‘blanket’ authorization attempting to cover all possible personal information and timeframes would not be appropriate.  |
| A credible threat has been received by college administration | Student's name and photo (possibly other relevant information for security purposes) | All Staff |   | The model for the care team is currently under development and once the model is complete, the determination of the level of threat will be assessed by the "Care Team". Information will be used, shared and disclosed on a "need to know" basis" to ensure safety. If timing permits, the disclosure decision should be supported by an assessment conducted by a qualified medical professional based on a full inquiry into the threat. A warning to others in the college community may be permissible, provided the "health and safety exception" is engaged. Notice of the disclosure must be provided to the person. |
| A college employee has collapsed at work and taken to the hospital and family must be contacted | Employee's medical status - e.g. Unconscious |   | Employee's Family and/or Doctor | The college may release this information. |