Personal Information includes the following:

- Address, phone number, fingerprints, blood type of an individual
- Info relating to the age, race, gender, ethnic origin, sexual orientation, marital/family status of the individual
- Info relating to the medical, criminal, employment history or financial transactions/status, educational status, educational history, student's grades and records and pictures/photos of a Student/Individual
- Social Insurance Number (SIN), employee number/student number (EMPL ID) or other identifiable number associated with an individual.
- Views or opinions of another individual about an individual (e.g. performance or other evaluation comments)
- Correspondence sent to the College by the individual that is implicitly or explicitly of a private or confidential nature and replies to that correspondence
- 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.

To reference the complete
Fleming Privacy Procedures

Visit the HOD Web Page at
http://fleming0.flemingc.on.ca/hod/FOI/FOIWelcome.htm
on the employee portal.

For questions contact the FOI Coordinator in the Human and Organizational Development Department at 705-749-5530

Privacy at Fleming

Understanding Your Responsibilities… as an Employee

Fleming College is committed to protecting the privacy of our students and employees.

Fleming College
Experience · Success

Your Responsibility as a College Employee

Freedom of Information and Protection of Privacy Act (FIPPA) came into effect for Ontario community colleges on January 1, 1989. This legislation specifies how Fleming College must handle personal information.

As a Fleming College employee you have a responsibility to understand what personal information is, and when working with personal information to collect, use and disclose it only where necessary to perform your individual job duties. You also have the responsibility to control, store and maintain it in a secure manner as to prevent unauthorized disclosure.

Individual college departments are responsible for developing and implementing their own guidelines and procedures to ensure that they reflect the intent of the privacy procedures and the FIPPA legislation

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

Collecting Personal Information:

The college will only collect and record personal information which is necessary for the administration of the college and its academic programs and ancillary services. On any forms which collect this information, the purpose for its use must be made clear to the individual.

Using Personal Information:

Personal information collected by the College will only be used according to our obligations under FIPPA. This will normally be for the purpose it was collected or related purposes the individual would have reasonably expected when providing their personal information.

Disclosing Personal Information:

Personal information will not be disclosed in most cases; however some very limited exceptions may apply. For example, to share personal information with a parent or future employer would require a written consent from the student. Consultation with the college FOI coordinator is recommended for other exemptions as needed.

Storing and Destroying Personal Information:

Employees are responsible for ensuring the security of personal information in their control. Records containing personal information must be stored in a secure manner. Hard copy files and records must be kept in locked filing cabinets within offices which are lockable outside of working hours.

Employees should always avoid copying and transporting college data which contains personal information onto laptop computers, PDA's, USB keys, and other external digital storage devices. If you must do this, you have the responsibility to keep it secure at all times.

When personal records are no longer required, they must be shredded or deleted from data devices as soon as no longer needed, to protect privacy.