UNIVERSITY OF CALGARY

ACCESS AND PRIVACY OFFICE

Frequently Asked Questions: General

Do I have to file a formal request under FOIP to access any or all information about the University of Calgary or about me?

No. The *FOIP Act* is in addition to and does not replace existing procedures for access to information or records. It should be seen as an instrument of last resort.

How do I file a request for information in the custody or under the control of the University of Calgary?

The FOIP Act is in addition to and does not replace existing procedures for access to information of records. A request for information that cannot be answered through existing procedures becomes a formal access request. A formal access request received anywhere on campus will be directed to the Access and Privacy Coordinator at the University Archives. *(please refer to the published procedures)*

How much will it cost to obtain personal information about myself?

An applicant who requests access to personal information about his or her self may be charged fees for copying the record in accordance with item 6 of Schedule 2 of the Act. Fees are charged only when the total amount exceeds $10.

How does the University determine whether an applicant's request for a fee waiver should be approved?

Section 97(4) allows the head of a public body to waive all or part of a fee if the applicant cannot afford the payment or for any other reason it is fair to excuse payment. The University can ask an applicant to provide information to support a request for such a fee waiver. It should address the issue of need for the information, alternative sources of the information and the reasons for the inability to pay. The President, Vice-Presidents, Associate V.P.s, Deans, Directors, the Registrar and the Access and Privacy Coordinator all have the authority to approve a fee waiver. The Access and Privacy Coordinator may also help the applicant narrow the request if necessary to reduce fees.

Is the University required to create a record from a record or data that is in electronic form?

Yes, in some circumstances. The University must create a record for an applicant if the record can be created from a record that is in electronic form using existing hardware and software and technical expertise. Fulfilling this obligation should not unduly interfere with the operations of the University.

When does the University notify third parties about information requests?

Section 30 sets out when the University must give notification to a third party. If the University is considering giving an applicant access to a record containing personal or business information of a third party, then notice must be given. The third party has 20 days to consent to disclosure or provide reasons why the record should not be disclosed. If access to the record is not going to be provided, notification is not required but is recommended as a courtesy unless it would be onerous.

Is it appropriate to circulate a monthly listing of FOIP requests, including the name of the requester, to unit FOIP Advisors?

No. It is not appropriate to reveal personal information about an applicant unless an employee needs to know that information in order to deal with the request. [Section 40(1)(h)] If the applicant is a business or organization, that information can be disclosed as only individuals have personal privacy rights. However, this practice is not recommended. A description of the request and the type of applicant can be circulated internally or provided to the Board.

What are the consequences for an employee of the University who destroys a record subject to a request with the intent to evade the request?

Destroying any record subject to the Act with the intent to evade a request for access is an offense and the individual is liable to a fine of not more than $10, 000. [Section 92(2)]

What are the consequences to the University if it does not comply with the FOIP legislation?

Apart from the embarrassment for a major public University in refusing to comply with mandated legislation of the provincial government and any resulting adverse publicity, the Information and Privacy Commissioner has the right to order compliance. In addition, the Act allows for fines up to $10,000 for individuals who:

- willfully collect, use or disclose personal information in violation of the privacy protection part of the Act,
- make a false statement to, or mislead the Commissioner, or his officers or any other person under the Act,
- fails to comply with a Commissioner's order, or
- destroys records subject to the Act with the intent to evade a request for access to the records [Section 92(1)(g)].

The Access and Privacy Coordinator will assist in ensuring that the University's collection, use and disclosure of information policies and practices comply with the legislation.

What is not considered to be an "unreasonable invasion of privacy" under FOIP?

It is not considered an unreasonable invasion of privacy if: the individual consents to the disclosure; an act authorizes disclosure; there are compelling circumstances affecting someone's health or safety; the personal information is about an individual who has been dead for 25 years or more; the information is about classification, salary range, discretionary benefits or employment responsibilities at the University; the information provides details of contracts (including financial) for the supply of goods and services to the University; or the information provides details of discretionary benefits or grants. (s*ee Section 17)*

Can the University use the SIN for student identification or as proof of citizenship?

No. The SIN should be collected only where the University is required to report income to the Federal Government or where legislation authorizes the collection for another purpose.

Can parents and potential students receive information on the performance of a school?

Yes. This is not a privacy issue, as the performance of individual students would not be released.

Can the University store personal information on computers in the United States?

The FOIP Act does not prohibit the storage of personal information in the United States. However, since the USA Patriot Act authorizes the warrantless seizure of personal information under conditions that may be objectionable to Canadians, there is some concern about personal information being on computers in the U.S. The University will, therefore, choose a local solution whenever possible.

When we make a business decision to outsource data management or data storage, the University must ensure that:

- the third-party provider can provide reasonable protection against such risks as unauthorized access, collection, use, disclosure, or destruction;
- the service agreement is specific about where the data will be stored, who owns the data, the circumstances under which the data can be accessed and/or used by the third party provider, what happens in the event of a security breach, and what happens when the service is no longer required; and
- clients are informed that their information may be processed by a third-party service provider.