

3.5) Confidentiality

All agents involved at St. Thomas University (i.e. faculty, staff, students as well as students employed as tutors and/or note takers) must treat all information pertaining to a student as confidential. The exceptions to this policy are:

- when an individual becomes aware of current children at risk of abuse
- when an individual clearly presents danger to self or others
- when we are subpoenaed for records or testimony by the courts

If a breach of confidentiality occurs then the individual is subject to disciplinary action.

Consent Forms

Consent forms must be signed by the students to disclose any information to any University staff and/or outside parties (such as family members or other individuals).

Consent forms are available at Student Accessibility Services.

¹Please contact Student Accessibility Services regarding the manual.

F. Policy Statement on Privacy and Protection of Information

i. When collecting and retaining information from prospective students, students, alumni, faculty, staff, and donors, St. Thomas University is subject to the Province of New Brunswick's *Right to Information and Protection of Privacy Act*, R.S.N.B. c. R-10.6 (the Act) and its regulations. The following policy statement should be read in conjunction with the *Data Steward Matrix* on Information and other documents which provide operational detail on the collection, maintenance, and security of information that is consistent with the Act and the University's services, programs, and activities.

Through its authorization to "continue, manage, (and) maintain" the University, the *Act to Incorporate Saint Thomas' College* empowers the University to gather information, including personal information, for activities related to its programs and administration. This would include, but is not limited to, recruitment, admission, registration, academics, degree granting, and advancement, as well as encompassing regular operational practices for faculty and staff:

i. Students

By applying for admission, students accept the University's right to collect information, including personal information, for the purposes of administering its services, programs, activities, or any other purpose consistent with its administration. Applicants agree that documentation they submit in support of the aforementioned activities becomes the property of the University.

ii. Faculty/Staff and Alumni/Donors

Other stakeholders — namely, faculty/staff and alumni/donors — are covered by this policy in accordance with the terms and conditions noted below and in their interactions with Human Resources, the Vice-President (Academic and Research), and the Deans of Humanities and Social Sciences, and Advancement and Alumni Relations.

Additionally, per Section 4 (h) of the Act, “teaching materials of an employee of an educational institution or other research information of an employee of an educational institution” are excluded from the application of the Act.

Policy Statement

St. Thomas University is committed to protecting the privacy of the information that it collects. Any individual sharing information with the University has the right to privacy regarding the collection, use, disclosure, retention, or correction of information as described in the Act subject to stated limitations and consistent with reasonable requirements for carrying out the services, programs, and activities of the University.

Collection and Use of Personal Information

The collection of personal information is necessary for the delivery of services, programs, and activities, with the amount of information collected limited to that which is necessary for carrying out these activities. When applying to St. Thomas University, providing information to Advancement, or initiating any other service or activity with the University, the individual is informed of the authority and purpose for the collection of the information and is provided with contact information with regards to any questions that may arise.

By providing information to the University, an individual is consenting to its use consistent with the purpose for which it has been obtained. The use and disclosure of personal information will be limited to the minimum amount necessary to accomplish the purpose for which is being collected. The custody, control, and access to the information is limited to those who need to know the information to carry out the purpose for which the information was collected. From time-to-time, the University will use information in order to highlight the success of the University and its students. Information may also be made available to federal and provincial authorities as required by legislation.

Any individual who has provided information to the University and believes that there is an error in that information may request a correction of that information.

Student Information

A student's record/file in whatever format, paper or electronic, is the official academic record used for processes related to admissions and academic performance. This record/file is the property of the University and, following application and admission, the Registrar's Office retains custody of the academic records and is responsible for security and maintenance. Other files may exist and relate to services or programming offered to students through the Offices of Athletics, Financial Services, Human Resources, Residence Life, Student Services, and Advancement. Relating to the Act, and as a guide for staff in their day-to-day operations, the information in a student record/file, whatever its location, is generally classified under two categories of information:

i. Public Information

St. Thomas University routinely makes institutional information available on its website. This aggregated information may include areas like the demographic composition, place of origin or permanent residence, graduation rates of students and/or information provided to the Maritime Provinces Higher Education Commission or analyzed internally by the Office of Institutional Research. If the information is not available, a request for

information may be made to the Privacy Officer and will be considered consistent with the provisions of the *Act*.

Beyond information that is published, the following information may be released without authorization: a student's degree or certificate conferred or to be imminently conferred and/or graduation date and the name of a recipient of a University scholarship, award, or other prize. A student may petition the Registrar's Office to restrict or deny access to this information.

ii. Confidential Restricted / Internal Information

Student information that is not public is considered to be personal information that is confidential and restricted and may not be released without authorization or written consent. This includes:

- whether the student is currently registered
- student record/file
- address/contact information
- grades/academic standing
- any identification information such as Social Insurance Number
- date of birth

Addresses and telephone numbers may only be used by University personnel to contact students about university-related matters or in emergency situations.

Staff who require access to student information in order to perform their duties are allowed access to the record or otherwise may request access to a record through a Data Steward, which is the administrator designated as being responsible for a body of information. Access to a record is permitted for carrying out duties for the purpose for which the information was collected or compiled or for a use consistent with that purpose. However, faculty do not normally have access to personal information beyond what is required for their teaching and faculty requests for other student information must be approved by the Registrar.

This Confidential Restricted/Internal Information is considered confidential and is not released to third parties external to the University except in emergency situations or with prior approval by the Data Steward and the Privacy Officer through application of the *Act*. (An emergency situation is defined by the *Act* as "if necessary to protect the mental or physical health or the safety of any individual or group of individuals" and applies generally to the public body.)

University students or external organizations may request lists which will only be approved if the addresses are to be used for a purpose that is consistent with the objectives of the University. Such requests should be submitted to the Privacy Officer for consideration who will consult with the Data Steward and consider the request through application of the *Act*.

Students have the right to obtain unofficial and official copies of their transcript of marks from the University. Request forms and any required fees must accompany the request to send an official copy of the transcript to another institution or employer.

Retention and Disposal of Personal Information

The Records Retention Schedule established by the University establishes the practices regarding the retention and disposal of records. The University is not subject to the *Archives Act* of New Brunswick.

Information Practices

St. Thomas University will have in place information practices (ie., policies for information management and retention, procedures, security arrangements, and response protocols) consistent with the *Right to Information and Protection of Personal Information Act* and its regulations (2010-111) and will require that its officers, staff, and faculty comply with security arrangements. The University will periodically test and evaluate the effectiveness of its information practices.

If there is privacy breach, St. Thomas University will follow the guidelines of the provincial regulations to investigate actual or suspected breaches, maintain a registry of breaches and corrective actions, notify a person or persons as soon as possible of a breach involving their personal information if it is reasonable that such a breach carries with it “significant harm” (determined by the sensitivity of information and probability of misuse) and notify the Commissioner.

Data Transfers

St. Thomas University retains the information, including personal information, that it collects on servers primarily located in New Brunswick but also in other locations. In addition, some payment information may be processed in the United States and may be subject to the privacy laws of the United States. St. Thomas will rely on legally-provided mechanisms to lawfully transfer payment information to the United States which may have data protection laws different to the laws of Canada.

Operational Direction

Nothing in this policy should prevent an employee from requesting clarification from their Data Steward or the Privacy Officer, as designated by the University, per the *Data Steward Matrix* on Information, particularly if there is a circumstance regarding disclosure of information to a third party.

Changes to Our Privacy Policy

St. Thomas University may change this Policy Statement from time to time to reflect changes in practices or in the applicable law. Where such changes are material in nature, St. Thomas University will provide additional notice such as adding a statement to our website.

Questions

Questions on privacy may be directed to the Privacy Officer, Jeffrey Carleton, Associate Vice-President, at privacyofficer@stu.ca.

Appendix I – Reference Definitions from Part 1 of the *Right to Information and Protection of Privacy Act*

“common or integrated service, program or activity” means a service, program or activity that is provided by a public body and one or more other public bodies or one or more non-public bodies

“educational body” means St. Thomas University and any faculties, schools or institutes

“employee”, in relation to a public body, includes an individual retained under a contract to perform services for the public body

“identifying information” means information that identifies an individual or which it is reasonably foreseeable in the circumstances could be utilized, either alone or with other information, to identify an individual

“information” means information contained in a record

“information practices” means the policies of a public body in relation to personal information, including (a) requirements regarding the collection, use, disclosure, retention, correction or disposal of personal information, including any requirements prescribed by regulation, and (b) the administrative, technical and physical safeguards and practices that the public body maintains with respect to the information, including any requirements prescribed by regulation

“personal information” means (edited list) recorded information about an identifiable individual:

- the individual's name
- the individual's home address or electronic mail address or home telephone
- information about the individual's age, gender, sexual orientation, marital status or family status
- information about the individual's ancestry, race, colour, nationality or national or ethnic origin
- information about the individual's religion or creed or religious belief, association or activity
- personal health information about the individual
- information about the individual's political belief, association or activity
- information about the individual's education, employment or occupation or educational, employment or occupational history
- information about the individual's source of income or financial circumstances, activities or history
- information about the individual's criminal history, including regulatory offences
- the individual's own personal views or opinions, except if they are about another person
- the views or opinions expressed about the individual by another person
- an identifying number, symbol or other particular assigned to the individual

“privacy breach” means any incident of unauthorized access, use, disclosure, or disposal of personal information in the custody of or under the control of a public body

“significant harm” includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record and damage to or loss of property

“record” means a record of information in any form and includes information that is written,

photographed, recorded or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces records

“third party” means a person other than the applicant or the public body