POLICY

Policy Title:	Information Privacy & Security		
Policy No:	6751	Policy Version:	1
		Approval Date:	**July 17, 2017**
Original Submission Date:	**July 17, 2017**	Effective Date:	**July 17, 2017**
Approval Body:	Academic Council	Revision Date:	**July 2019**

Policy Statement

At Acsenda School of Management (ASM), we are committed to providing our students, employees, alumni, donors, research participants, retirees, and others with exceptional service. As providing this service involves the collection, use, and disclosure of some personal information about our students, employees, alumni, donors, research participants, retirees, and others (subsequently referred to as members), protecting their personal information is one of our highest priorities. We are committed to excellence in the management of this information.

We will inform our members of why and how we collect, use and disclose their personal information, obtain their consent where required, and only handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

This Personal Information Protection Policy, in compliance with PIPA, outlines the principles and practices we will follow in protecting members' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of our members' personal information and allowing our students, employees, alumni, donors, research participants, retirees, and others to request access to, and correction of, their personal information.

ASM upholds the definition of personal information as specified under the Personal Information Protection and Electronic Document Act (PIPEDA) and the BC Provincial Information Protection Act (PIPA).

Purpose

To ensure that ASM protects the privacy of its members whose personal information is in ASM's custody or control and that it upholds applicable privacy legislation governing the collection, use, and disclosure of personal information.

Scope

All campuses and organizational units of Acsenda School of Management. All information and records in the custody and/or under the control of ASM. The policy is based on the requirements of the privacy legislation that applies to ASM. In order of importance for Institutional operations, the two Acts that apply are:

- the Provincial Personal Information Protection Act (PIPA)
- the Federal Personal Information Protection & Electronic Documents Act (PIPEDA)

Acsenda School of Management complies in all respects with all applicable privacy legislation and other applicable privacy legislation that may be enacted.

All employees of ASM are responsible for the protection of the privacy of students, employees, alumni, donors, research participants, retirees, and others whose personal information is in the custody and/or

under the control of ASM. All employees are expected to undertake privacy awareness training authorized by ASM.

The President has ultimate accountability for compliance with privacy provisions. The President may delegate his or her powers under in whole or in part, but his or her delegates may not sub-delegate. The delegation of the President shall be in writing. Delegates may assign related duties to subordinates as necessary to fulfill delegated responsibilities.

Department heads are responsible for establishing and maintaining measures to ensure their units are protecting privacy, in accordance with the Privacy Policy and application privacy legislation.

ASM Privacy Officer is guided by Acsenda School of Management's Privacy Policy in executing her/his responsibilities.

In compelling circumstances, for example where health and safety may be at stake, disclosures of personal information may be made in accordance with exceptions for such circumstances in the legislation. Employees considering disclosure of personal information in such circumstances must seek advice from ASM Privacy Officer. If this is not possible during an emergency, employees must take reasonable measures to protect personal information.

Acsenda School of Management is guided by the following principles:

a. **Accountability:** ASM is responsible for personal information in its custody and/or under its control and has designated a Privacy Officer who is accountable for the organization's compliance with these principles.
b. **Identifying Purposes and Consent:** ASM identifies to the individual the authority and purposes for the collection and use of personal information at the time of collection, and the contact information of an employee who can answer questions about the collection. ASM obtains the individual's consent to the collection of sensitive personal information and personal information collected for the purpose of disclosure outside ASM. ASM collects personal information directly from the subject of the information whenever it is feasible and appropriate to do so. When direct collection is not feasible or appropriate, ASM makes every reasonable effort to ensure the accuracy of personal information collected from third parties.
c. **Limiting Collection:** ASM limits its collection of personal information to that which is required for its programs and services. Wherever feasible and appropriate, ASM collects personal information about students, employees, alumni, donors, research participants, retirees, and others directly from the individual concerned. A Privacy Notice is provided to the individual at the time of collection.
d. **Limiting Use, Disclosure, and Retention:** ASM limits its use and disclosure of personal information to those purposes in accordance with the applicable privacy legislation. ASM uses personal information only for the purpose for which it was collected or compiled; for a consistent purpose; with the written consent of the individual; or for the purpose for which the information was disclosed to ASM. Employees collect and use only the minimum amount of personal information needed. ASM does not disclose personal information to any individual other than the subject unless it is permitted under PIPA/PIPEDA. Any disclosure is limited to the minimum amount necessary.
e. **Accuracy:** ASM makes every reasonable effort to ensure that the personal information it collects, uses, and discloses is accurate and complete. Each individual is responsible for ensuring his/her information is correct and current.
f. **Security:** ASM ensures that personal information in its custody is secured in a manner appropriate to the sensitivity and purpose of the information. ASM ensures that records containing personal information are protected from unauthorized collection, access, use, disclosure, and disposal by putting in place reasonable administrative, physical, and technical security measures. All employees ensure that personal information which they handle as part of their job is secure from unauthorized

access, that collection, use and disclosure of personal information is minimized and that records are managed in accordance with an established records retention and disposal system.

g. **Openness:** ASM's Privacy Policy and related procedures are available on ASM's website at http://www.acsenda.com/about-us/privacy-policy/ and this on-line version is the official version. Printed copies are available from ASM Privacy Officer, who responds to any related questions. ASM notifies affected individuals of any potentially detrimental breaches of its privacy controls in accordance with the PROCEDURE FOR NOTIFICATION OF A PRIVACY BREACH.

h. **Individual Access:** An individual may access his or her personal information by making a written request to ASM department responsible for the information, or to ASM Privacy Officer. ASM may require an individual to prove his/her identity before providing access to his/her information. A fee may be levied if the request requires the use of extra personnel or University resources. When personal information is used to make a decision affecting someone, the information will be kept for at least one year so that the individual will have sufficient opportunity to access the information, if desired. Upon request from an applicant, ASM will correct an error or omission in an applicant's personal information or annotate the file if no correction is made.

i. **Challenging Compliance:** Complaints or questions with respect to ASM's compliance with this Privacy Policy must be directed to ASM Privacy Officer. ASM Privacy Officer shall investigate all complaints received or shall delegate the investigation to another investigator.

To monitor compliance with the Privacy Policy, all projects involving personal information must be reviewed by ASM Privacy Officer. This compliance requirement does NOT apply to research projects involving human participants, which have received ethics approval from a duly-constituted research ethics board, including a research ethics body.

Noncompliance

1. University employees who act in good faith and who execute their employment responsibilities with a reasonable standard of care shall not be subject to discipline for unintentional privacy breaches.

2. Privacy breaches arising from noncompliance with the legislation or this policy may result in disciplinary action up to and including dismissal.

Definitions

These definitions apply to terms as they are used in this policy:

Word/Term	Definition
Legislation	The privacy legislation with which ASM is required to comply. Depending on the nature of the personal information and the purposes for which it is collected, used or disclosed, the legislation may be one or more of the Provincial Personal Information Protection Act (PIPA) or the Federal Personal Information Protection & Electronic Documents Act (PIPEDA)
Personal Information	Means recorded information about an identifiable individual, including (but not limited to) • the individual's name, address or telephone number • the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations • the individual's age, sex, sexual orientation, marital status or family status • an identifying number, symbol or other particular assigned to the individual • the individual's fingerprints, blood type or inheritable characteristics

	• information about the individual's health care status or history, including a physical or mental disability • information about the individual's educational, financial, criminal or employment status or history • the opinions of a person about the individual, and • the individual's personal views or opinions
Privacy	The protection of the collection, usage, storage, destruction, and dissemination of personal information on alumni, donors, students, staff, faculty, and ASM stakeholders.
Privacy Breach	Occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information
Record	A record of information in any form and recorded or stored in any manner, including paper, electronic, digital, audio, and video, but does not include a computer program or a mechanism that produces records on any storage medium
University Privacy Officer	The position with overall management responsibility for privacy policy and procedures at ASM. *This is a functional description, not a title*. ASM Privacy Officer is appointed by the President of ASM.

Related legislation

- the Provincial Personal Information Protection Act (PIPA)
- the Federal Personal Information Protection & Electronic Documents Act (PIPEDA)

Related policies

Policy Number	Policy Title
6750	ASM Records Management Policy
5011	Research Ethics

Responsibility

Duties of the Privacy Officer

- All personal information inquiries or complaints fall under the jurisdiction of ASM Privacy Officer.
- Members of ASM and ASM staff may request access to their personal information and may request corrections to personal information so that it is complete and accurate.
- ASM Privacy Officer will ensure the protection of personal information safeguarded by ASM including:
    - Limiting access to personal information to those employees who require access to the information in the performance of their job function;
    - Installing and maintaining reasonable security safeguards to prevent unauthorized access of its computer system and hard copy files;
    - Not collecting or disclosing personal information for purposes other than what is listed in this policy;
    - Ensuring that personal information kept is accurate and current; and
    - Destroying personal information (when required) in a manner that maintains the confidentiality of that personal information.

PROCEDURES

Action Required	Position Responsible	Action Required
1. Contain the breach.	Program area where breach occurred.	Immediate
2. Report the breach within the organization or public body	• Program area staff (report to management) • Management • Privacy Officer	Same day as breach discovered
3. Designate lead investigator and select breach response team as appropriate	Privacy Officer	Same day as breach discovered
4. Preserve the evidence	Lead Investigator or Privacy Officer	Same day as breach discovered
5. Contact police if necessary	Privacy Officer	Within 2 days of breach discovery
6. Conduct preliminary analysis of risks and cause of breach	Lead Investigator	Within 2 days of breach discovery
7. Determine if the breach should be reported to the Privacy Commissioner	Privacy Officer in consultation with executive	Generally within 2 days of breach
8. Take further containment steps if required based on preliminary assessment	Lead Investigator or Privacy Officer	Within 2 days of breach
9. Evaluate risks associated with breach	Lead Investigator or Privacy Officer	Within 1 week of breach
10. Determine if notification of affected individuals is required	Privacy Officer	Within 1 week of breach
11. Conduct notification of affected individuals	Privacy Officer or program area manager	Within 1 week of breach
12. Contact others as appropriate	Privacy Officer or program area manager	As needed
13. Determine if further in-depth investigation is required	Privacy Officer or program area manager	Within 2 to 3 weeks of the breach
14. Conduct further investigation into cause & extent of the breach if necessary	Privacy Officer, security officer or outside independent auditor or investigator	Within 2 to 3 weeks of the breach
15. Review investigative findings and develop prevention strategies	Privacy Officer or program area manager	Within 2 months of breach
16. Implement prevention strategies	Privacy Officer or program area manager	Depends on the strategy
17. Monitor prevention strategies	Privacy Officer or program area manager	Annual privacy/security audits

APPENDICES