*The University of Regina (the "University") is a local authority subject to The Local Authority Freedom of Information and Protection of Privacy Act (the "Act") and regulations. As an **employee** of the University, **you are obligated to protect** the personal and/or personal health information collected by the University from and relating to its students, faculty, staff, and others.*

What is considered personal information?

***Personal information* is information about an identifiable individual**. Examples include, but are not limited to, information related to race, religion, colour, sexual orientation, family or marital status, disability, age, nationality, education, employment, health, identifying #, address, etc.

Can I use and disclose personal information?

As an employee of the University, if you require personal information of students, faculty, staff or others to perform your role or provide services to an individual, you may collect, access, use, retain and disclose personal information in accordance with the Act. However, **"snooping" is not allowed** - you cannot collect, access, use, retain or disclose personal information out of curiosity or for unauthorized or unnecessary reasons.

What student information can I share with others?

The personal information of students should only be shared with relevant students themselves (as in the case of student grades) and those that need it to do their jobs at the University. Even then, only the minimum amount of information necessary for an authorized purpose should be shared with those that need to know.

The personal information of students should **not be shared outside of the University** (including with parents, family members or friends), except in the rare case where the student has provided authorization for such access. If a student indicates that such permission has been provided, please contact the Registrar's Office to confirm.

What should I do to protect personal information?

- Lock filing cabinets containing files that include personal information.
- Ensure your passwords are "strong" and changed frequently by using the University's Password Guideline assessment tool.
- Do not share your password or other system credentials.
- Take Information Services' Information Security Awareness Training.
- Put a password protected screen saver on your computer monitor so that no one can access your system in your absence. Lock your screen when you are away from your desk.
- Double check and reconfirm accuracy. i.e.: When assisting a returning student or customer – double check that their email, phone number, and address details are current and correct.
- Records containing personal information should not be discarded or recycled – they should be confidentially shredded. Hard drives or devices containing personal information must be professionally "wiped" by Information Services.
- Add a privacy disclaimer at the bottom of your e-mail. Here is an example for your use:
    This e-mail message is privileged and/or confidential and is only for the intended recipient(s). If you have received this message in error, please advise the sender by return e-mail immediately, and permanently delete this message.
- Contracts: Please note – 'Legal review is mandatory for most contracts prior to obtaining an authorized signature.' Contact our Governance Office prior to signing!

What happens if there is a breach of privacy?
If you are aware of a breach of privacy, such as an inadvertent sharing of someone's personal information by email or other means, you are required to immediately notify the Privacy Head. Please refer to Reporting a Privacy Breach.

I want to install or purchase new software to engage UofR students, potential students or staff?

- Contact IS Help Desk and complete an IS Technology Risk Assessment Intake form. This is an inclusive approach to evaluating the potential purchase or requests for additions/changes to information services. It is a quick analysis for risk, privacy implications, compliance, business continuity and organizational fit. Most importantly it assesses the protection of privacy of those who work or study here and encourages a proactive approach to privacy impacts.

Where can I find more information and training related to the Protection of Privacy?
- Visit our webpage: Privacy and Access
- Review the *University of Regina's Freedom of Information and Protection of Privacy Policy*
- Sign up for the University's privacy workshops when offered
- Check out: SK Privacy & Access 4-part course: basic awareness of access & privacy legislation

If you have any concerns or questions please contact:

Avneet Nehel	Patty Niebergall
Contract & Compliance Advisor	Privacy & Protocol Officer
Email: privacy.access@uregina.ca	