

Privacy at the University of Alberta – Highlights and Quick Tips

From the Information, Privacy and Records Management Office (“IPRMO”)

Here are some highlights and quick tips on how to protect personal information while working for the University of Alberta. For more information, please see the [IPRMO website](#).

As a university employee, you may come into contact with sensitive or confidential information including “personal information” such as student, employee or health information. Protecting personal information at work is essential. Here are some important tips to protect this information:

1. Respect privacy. The University must respect and protect privacy to fulfill its legislative requirements and maintain the fundamental bond of trust with the employees and students it serves.
2. Only collect, use and access the least amount of personal information to perform your duties. Ask yourself, is this something “I need to know” or is it “nice to know”? For example, if you only need an age range, collect that instead of birthdates.
3. Before you collect personal information directly from the individual the information is about, you need to notify them of the purpose of collection including how the information will be used. Whenever possible, collect an individual’s personal information from them directly, and not from someone else. For additional information about the collection of personal information under the *Protection of Privacy Act* ([POPA](#)), please visit the [IPRMO website](#).
4. Only disclose personal information if it is consistent with why you collected it, if you have the individual’s written consent, or as otherwise authorized by law. Only disclose the least amount of information necessary. Authorization and consent template forms are available on the [IPRMO website](#)
5. Just because you have access to personal information because of your job, it doesn't necessarily mean you have authority to access and use it for any purpose, particularly just for the sake of curiosity. Only access personal information if/when it is necessary for and directly relates to your job responsibilities.
6. Take reasonable steps to make sure that personal information is accurate and complete before you rely on it to make a decision that affects them or someone else. Individuals have the right to request a correction to any inaccurate personal information held about them.
7. If you use an individual’s personal information to make a decision about them, you have to keep it for at least a year.
8. Protect personal and/or confidential information according to the level of sensitivity of

the information. The more sensitive the information, the more [safeguarding](#) should be applied.

9. Retain and dispose of personal information records in a secure manner. For additional information, visit the IPRMO's [Records Management page](#). Make sure you securely wipe electronic devices, shred paper records when disposing of them, and never dispose of personal information in regular garbage or recycling bins.
10. Safeguard personal information by doing the following:
 - Limit access to those who need to know.
 - Don't discuss personal and/or confidential information in public areas.
 - Protect your user IDs (including CCID) and passwords. You are responsible for all actions undertaken with your user ID. Do not share your password.
 - Encrypt digital records - you must encrypt mobile devices that access and/or store university records
 - Remember that [email](#) may not be the most secure way to transmit personal or confidential information (consider level of sensitivity); sharing a document via [Google Drive](#) may be a more secure method.
 - Transport and transmit the minimum amount of personal information necessary.
 - Transport and transmit personal information securely by using locking devices and keeping devices or information with you at all times (do not leave university records or mobile devices in your vehicle if left unattended).
 - When e-mailing, double-check addresses to be sure you are sending it to the correct individual. When emailing a group of people, put email addresses in the "bcc" line instead of the "to" or "Cc" lines.
 - Lock your computer when you step away from your desk and log out of applications when you leave work for the day.
 - For additional information, please see [safeguarding personal information](#) and [Email + Phishing](#).
11. Report [Privacy and Information Security incidents](#) as soon as possible.
15. University employees must complete the mandatory Online [Privacy and Security Training and Acknowledgement](#) at the time of hire, acknowledge annually and refresh the training every three years. Privacy and security related information and guidance changes - refresher training is important!