Privacy Pitfalls at UBC

All UBC staff and faculty members are subject to the Freedom of Information and Protection of Privacy Act (FIPPA), which contains strict rules about the collection, use and disclosure of personal information. Here, in no particular order, are some of the main privacy pitfalls we commonly encounter at the University:

- **Collecting personal information when it's not necessary.** Personal information should only be collected if it is necessary for an authorized UBC program or activity. Sometimes, we collect personal information when it's not really necessary to do so.
- **Disclosing personal information without authority.** Before disclosing personal information, stop and think: do you have authority to do so? If you're not sure, talk to the Access and Privacy Manager.
- **Emailing personal information.** Emails are not a secure method of communication. While it is acceptable to include small amounts of non-sensitive information in your emails, larger volumes of personal information should be protected by placing the information in an Excel or Word file and encrypting it. IT Security can provide more information about encrypting files.
- **Storing personal information on a mobile device.** Laptops, smartphones, USB drives and CDs are easy to lose or steal. If you are storing unprotected personal information on these devices, you are asking for trouble! Therefore, it is highly recommended that you encrypt the information. IT Security can provide more information about encrypting devices.
- **Using cloud services.** Cloud services are computing and data storage services delivered via the internet (eg. Dropbox, Hotmail, Google Docs). As a rule, you must not use these services to store or transmit personal information because this violates privacy and security requirements. There are exceptions to this rule, which the Access and Privacy Manager can discuss with you.