REB Guidelines for the Storage and Use of Personal Data obtained through Research.

Purpose:

These guidelines highlight the general issues that the Research Ethics Board (REB) of Concordia University of Edmonton (CUE) wants you to consider when storing and using information about living, identifiable individuals that pertain to your research. These guidelines apply to personal information in both paper and electronic formats to ensure that this information is kept secure, and that CUE complies with its obligations under Alberta's *Personal Information Protection Act* (*PIPA*) as well as the *Tri-Council Agreement*.

Who is this for?

These REB guidelines apply to for all faculty, staff members, researchers, research assistants, and students who store personal information through their research activities at CUE. These guidelines also apply to all documentation related to your research (i.e. paper documentation, word processed documents, spreadsheets, databases and e-mails) which contain personal information and which can be found on and accessed via various devices such as your desktop, laptop PCs, PDAs, mobile telephones, USB memory devices, CDs and DVDs.

Why should You be concerned about this?

PIPA applies to all "personal information" about a living, identifiable individual. It sets out how we should use this information. Those conducting research must take reasonable measures to protect personal information from risks such as unauthorized collection, use, or disclosure. Failure to comply with *PIPA,* CUE's Personal Information Protection Policy (*PIPP*), and these guidelines could expose you and CUE to legal proceedings or reputational damage.

The definition of personal information is complex. For day-to-day purposes it is best to assume that all information about a living, identifiable individual is personal information.

A) General Guidelines

1) Familiarize yourself with CUE's *PIPP*. Follow its guidelines and practices in how you collect, store, use, distribute and destroy personal information when conducting your research.
2) Anonymise personal information whenever possible.
3) Don't assume that information has been anonymised just because you have removed names – electronic codes may still link the information to particular individuals, or they could still be identified from the data that remains, for example a combination of department, ages and gender.
4) Use encryption, access permissions and other features to restrict access to personal information to staff who need to see it to do their job.
5) Always encrypt the data and ensure that physical devices cannot be accidentally lost (i.e., by not leaving the device unattended).
6) Be careful when embedding documents - when you embed a document it is possible for the reader to access the entire document and not just the information on display.
7) Laptops and other electronic devices such as PDAs should be password protected. Access to personal information should be password protected, including when stored on a password-protected storage device such as floppy disk, CD, or USB storage drive, rather than the hard drive of your laptop or home computer. Choose a password that is not easy to guess.
8) Don't share passwords.
9) Don't write your password down. If you must write it down then don't store it in an easily accessible place.
10) Don't assume that e-mail is a private or secure form of communication. Avoid using e-mail to transmit personal information.
11) Don't send someone's username and password in the same e-mail or document; send them under separate cover.
12) Delete personal data as soon as it is no longer required. Do not store personal information for time periods longer than those recommended by the REB unless the REB has consented to this.
13) Ensure that your deleted items are actually deleted – simply deleting items does not always remove them completely from you computer. For example, in Microsoft Outlook when you delete e-mails they are moved to and stored in your 'deleted items' folder and you must also delete them from here. Similarly in Windows when you delete items from your computer they will often be sent to the 'recycle bin' on your desktop, from where you must delete them again.
14) Take particular care when disposing of or selling a PC or any other device that potentially holds personal data – ensure that all personal information has been deleted.

15) Ask CUE's IT support service for advice on making your computer and your information secure.

B) Best practices of physical security measures:

1) Control the distribution and return of keys to those areas where personal information is stored. If necessary, make changes to locks to prevent inappropriate room entry. Take action if you suspect that unauthorized staff have accessed personal information.
2) Lock doors and filing equipment when the office is vacant.
3) Site PCs where the screen cannot be seen by unauthorized staff, students or the public. Don't leave information on the screen when you are not there – have your screensaver set to activate quickly if you leave your computer unattended.
4) Ensure that sensitive and confidential information is not visible to the public. Encourage a clean desk policy to reduce the risk of exposing confidential information to others.
5) Label filing cabinets, drawers, boxes and other storage containers in a manner that maintains the anonymity of items in storage.
6) Where possible, modify office layout to protect confidential information from inappropriate exposure.
7) Lock your computer, if possible, if you are leaving your desk for more than 5 minutes.
8) Ensure confidential destruction of paper records by using a cross-cut shredder or by placing the records in one of CUE's locked boxes designated for cross-cut shredding.

C. Protecting Personal Information Outside the Office

1) Never travel with personal information unless you absolutely must have it with you. If you take personal information with you, take the least amount that you need and leave the rest behind in a secure location. If possible, you should only take copies, leaving original documents in the office.
2) Take appropriate security precautions if you take any information about people home with you. Make sure it cannot be accessed by thieves or accidentally viewed by visitors or family members. Access should be password protected.
3) While away from your office or your home, laptops and other electronic devices containing personal information (including PDAs such as Palm Pilots and Blackberrys) should be kept with you. If you must leave a laptop or other device somewhere, make sure that it is

in a location secure from theft, loss and unauthorized access to personal information. Set the automatic logoff to run after a short period of idleness. Protect your laptop by using locks or alarms as appropriate.

4) Don't share a laptop for working with private information with other individuals, including family members or friends.
5) If the records you need are too voluminous to carry with you, send them to your destination by a trustworthy courier.
6) You should avoid viewing or discussing personal information in public, including while traveling on airplanes, trains, buses and public transit.
7) When in transit or working outside the office, avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard and can be intercepted.
8) Don't leave records containing personal information in plain view in your hotel room.
9) Records containing personal information when locked vehicles have been broken into or the vehicle has been stolen. Records should only be left in the trunk of a vehicle if there is no other option, and only for a very brief period of time (less than one hour).
10) You should avoid sending personal information by email or fax from public locations, including internet cafes.
11) Upon returning to the office, return records to their original storage place as soon as possible or destroy the copies securely. Any working notes that you have created during that trip and which contain personal information should also be stored in a secure environment as soon as possible.
12) If personal information is stolen or lost, immediately notify the Privacy Officer for CUE and also the chairman of CUE's REB.

D. Transmitting Personal Information Across the Border of Alberta

If, in the course of your research, it becomes necessary for you to transmit personal information across the Alberta border, please contact both the Privacy Officer of CUE as well as the chairman of CUE's REB before transmitting such information. In such cases it will be necessary to ensure that the transmission of the personal information complies with the Government of Canada's *Personal Information Protection and Electronic Documents Act* as well as the privacy legislation of the jurisdiction to which the personal information is transmitted.