UNIVERSITY OF
CALGARY

University Policy
University Procedure
Operating Standard
Guideline/Form

Dealing with Confidential Records

1. Defining a Confidential Record

A confidential record is a record that contains information whose unauthorized disclosure could be prejudicial to the interests of the University.

A record is confidential if it includes:

- information about an identifiable individual that is not available in published or public sources or is not considered to be a matter of public record;
- information relating to the business of the University that is not already in the public domain;
- information about a organization or individual associated with the University that is not already in the public domain and which may contain commercially sensitive information;
- information that is subject to any type of legal privilege; or
- information that was supplied either explicitly or implicitly in confidence.

Some confidential information is only sensitive for a short period of time. For example, a press release is considered confidential until the designated release date and time. Other information will be considered confidential for longer periods. For example:

- proposed plans, policies or projects may have a limited distribution until a decision has been made;
- some types of personal information may not be disclosed until the individual the information is about has been dead for 25 years.

When information is supplied to the University by a either explicitly or implicitly in confidence, the expectation that it be kept confidential

2. Creating a Confidential Record

Be explicit about your expectations with respect to the dissemination of the information or distribution of the record by indicating on the document itself that it is to be considered confidential. You should also be clear about who is privy to the information.

For example: Confidential – Circulate to committee members only

3. Working with Confidential Records

To ensure that confidential information is not inadvertently disclosed:

- position your computer screen so unauthorized persons are not able to read it;
- engage a screen saver, turn off the monitor, or close down the program when you are interrupted;
- turn off your computer when you will be away from it for a long period of time;
- have password access to your computer and ensure your password is secure;
- place copies of records in folders or envelopes, out of sight of the general public;
- place drafts and final versions in locked file cabinets when you are not working on them for a period of time;
- shred drafts once they are no longer useful;
- delete drafts from your computer once they are no longer useful;
- have access to your work area restricted by a physical barrier.

4. Travelling with Confidential Records

Ensure that you:

- take only what you absolutely need in either paper or electronic format;
- carry the records in a locked briefcase or carrying case;
- do not leave your Personal Digital Assistant (PDA) in a jacket pocket or external pocket of your baggage;
- if the records are too voluminous, consider sending them ahead via a secure courier;
- keep the records or your laptop with you at all times - do not leave them unattended in an unlocked office or meeting room;
- do not leave records or your laptop in an unlocked vehicle or on the seat where they are visible to passersby;
- do not leave records or your laptop unattended in a hotel room. If necessary, use the hotel safe;
- consider using removable storage cards to prevent the loss of data if your PDA or laptop is stolen. Keep removable storage media in a separate location from your PDA or laptop when not in use while traveling;
- return the records to their original secure storage place upon return;
- if you need to look at the records while en route, prevent others from being able to read them;
- prevent unauthorized access to the operating system by password protecting your laptop or PDA operating system;
- encrypt electronic data;
- use anti-virus and firewall programs to protect your laptop or PDA;
- enable all safety protocols and ensure that you are using a secure wireless connection whenever you make use of a wireless network with your laptop or PDA;
- disable Bluetooth and Wi-Fi software whenever you aren’t using your wireless connections;
- use programs to monitor and detect activity on your PDA;
- notify your supervisor, the FOIP Coordinator, and campus security if a theft occurs.

5. Faxing Confidential Records

Ensure that you:

- include a fax transmittal cover page with a confidentiality statement;
- confirm that the information is being transmitted to a fax machine in a secure location with controlled access or that the material will be secured upon arrival;
- visually check the number displayed on the screen for accuracy before proceeding with the transmission;
- confirm receipt of the material by calling the recipient after transmission or by having the recipient call you when the fax is received, if possible;
- notify the sender and return or destroy the information if you receive a transmission in error;
- check the number of pages received against the number sent;
- locate your fax machine in a secure area with controlled access.

6. Storing Confidential Records

Confidential records should be stored in a secure location to ensure that no unauthorized persons will have access to the information. Secure locations include:

- locked filing cabinets
- record centre in a locked room
- secure servers

7. Destroying Confidential Records

All records containing confidential information must be shredded in accordance with established policy and procedures.

Remember that any records set aside for confidential shredding must be held in a secure area until they are shredded or picked up.

For further information, please contact the FOIP Coordinator at foip@ucalgary.ca.