360 GSP Training

POLICIES, RULES AND PROCEDURES

Confidentiality Policy

Policy Last Reviewed on: 01/12/2017

CONFIDENTIAL RECORDS Information and Privacy Guidelines

1. Defining Confidential Records

1.1 What is a confidential record?
Confidential records contain information that for one or more reasons should only be disclosed to specific people or groups.

1.2 What kinds of records could be considered confidential?

(a) Information relating to the business of a third party which is

- a trade secret or scientific, technical, commercial, financial or labour relations information, and
- supplied in confidence, implicitly or explicitly, and
- result in harm to competitive or negotiating position;
- result in information no longer being supplied;
- result in undue loss or gain, or
- reveal information supplied to or the report of a conciliation officer, mediator, labour relations officer or other person appointed to resolve a labour relations dispute.

(b) Personal Information

- Personal information (information about an identifiable individual) should be treated as confidential unless it is public information or unless there is consent for disclosure from the individual.

(c) Solicitor-client privilege

- Information that is subject to solicitor-client privilege, or that is prepared by legal counsel for use in giving legal advice or in contemplation of or for use in litigation.

(d) Other types of confidential records

Other types of records might need to be treated as confidential, depending on the content and circumstances. These include but are not limited to:

- Law enforcement information/proceedings (may include administrative tribunals, student disciplinary proceedings, etc.)
- Government relations information
- Information related to economic interests
- Institutional plans
- Tests or examinations
- Closed meetings

1.3 When could records cease to be confidential?
Some confidential information is sensitive for specified periods but may cease to be confidential after a certain period of time or change of circumstances. Here are some examples:

- A press release would be considered confidential until the release date and time.
- Institutional plans, policies or projects would be considered confidential while in development. Once a decision has been made on them and they are disclosed broadly, they could cease to be confidential.
- Personal information is always treated as confidential unless it is about a person who has been dead for more than 30 years.

2. Identifying and Labelling Confidential Records

It is important to treat confidential records differently from those which are more broadly distributed. Confidential records should be labelled so that they are easily identifiable.

- Ensure that records for which circulation should be limited are clearly marked CONFIDENTIAL.
- Determine who should have access to a confidential record. Normally a College employee who needs the information in performance of his/her duties would have access. For example, a member of a committee considering someone for an award would have access to the committee's record of proceedings but circulation would be limited to committee members only and held in confidence.

- Note on the record itself or in associated notes the persons or groups who should have access to this information, e.g. Confidential – circulate to committee members only.

- Use the “confidential” designation thoughtfully. Don’t mark most or all of your records as CONFIDENTIAL. Doing so will undermine the argument for treating selected records as confidential.
  And, while a confidential marking does not mean that a record will not be disclosed as the result of an access request, it may help to explain if the College makes a decision not to release a record in response to a request for access to it.

3. Working with Confidential Records

Ensure that confidential information is not inadvertently disclosed:

- Position your computer screen so that no unauthorized persons can read it.
- Close down the program or use password protection on your computer when you leave your desk.
- Turn off your computer when leaving your desk for a long period of time.
- Place paper copies of drafts and final versions in locked file cabinets when you are not working on them.
- Shred drafts when they are no longer useful, and delete drafts from your computer
- If you have confidential records on a notebook or laptop computer, ensure that the documents themselves or the system is password protected. Don’t leave your laptop in an easily accessible area where it could be stolen.
- When travelling with confidential records, don’t leave them unattended in vehicles, hotel or meeting rooms. Don’t work with confidential records where others can see them.
- When faxing confidential records, include a fax transmittal page with a confidentiality statement. Verify that the number on the screen is accurate before proceeding with the transmission, and confirm receipt of the documents.

4. Storing Confidential Records

Ensure that confidential information is protected against unauthorized access. Confidential records must be stored in a secure location such as a locked file cabinet, locked record room or on a secure server.

Don’t store confidential records in storage space which is shared with other units.

5. Disposing of Confidential Records

Dispose of confidential information securely and ensure that any personal information to be destroyed has been authorised for disposal.

At 360 GSP College, acceptable methods to dispose of confidential records are:

- Shred documents in an office paper shredder. Cross-cut shredders are preferred over strip shredders.
- Place documents in a locked confidential disposal bin obtained from Admin When full, make request for pick to Admin. Filled confidential bins are held in a secure area until contents are shredded on site.
- For electronic media such as floppy disks, CDs, USB keys, personal digital assistants (PDAs) and hard drives, destroy electronic records by overwrite software or physical destruction of disk, drive or other digital storage media. Note that overwriting may not irreversibly erase every bit of data on a drive.

This document has been developed to assist in establishing good practices and procedures. Additional questions or requests for advice on records and information management or information and privacy issues should be referred to the College Coordinator.