CONFIDENTIALITY POLICY

Confidentiality and Information Security Policy

The purpose of this document is to establish and promote the ethical, legal, and secure use of all information including computing and electronic communications for all members of the MUWCI ("**College**") community.

Security and confidentiality are matters of concern to the entire College as all members (including, without limitation, employees, consultants) have access to various records either in hard copies or via electronic or micrographic media. Every member of the College who has access to these records/information including, but not limited to, personal records, labour relations issues, proposals, bids, quotations, donor information and any other confidential information as it relates to the College and the relationship between the College and its donors and constituencies is responsible for the accuracy, integrity and confidentiality of these records). The purpose of this policy is to ensure that this responsibility is fulfilled and to clarify responsibilities of all members.

All members with access to information are in a position of trust. They are required to understand and abide by a high standard of behaviour and not to disclose information to any third party or to use it for any purpose either during employment/ engagement, except as may be necessary in the proper discharge of their duties, or after termination for any reason, except with the written permission of the College. The requirements documented in this section describe three key principles that help maintain security of sensitive information and data. All members of the College who have access to such information as mentioned above are expected to comply with the key principles:

1. Act in ways that protect sensitive data/information about the institution, the students and other members;
2. Use the data/information for authorized purposes only, as authorized by the College management;
3. Use the College's communication systems in an appropriate manner.

For the purposes of this policy," information" also includes but is not limited to files, documents, records (including electronic records), or any other materials, maintained, stored, controlled, or possessed by the College or any knowledge learned through employment/ engagement with the College. All notes, data, correspondence and other records, whether paper or electronic, and other materials in any way relating to any of the College records or to the College's business produced by members or coming into their possession by or through their employment or engagement shall belong exclusively to the College, and members agree to turn over to the College any such materials in their possession or under their control forthwith, upon the termination of their employment/ engagement with the College.

Information Access and Sharing- "Need to know"

Members may receive proprietary information relating to the College in the course of their work and are obligated to protect such information from disclosure. They must disclose information only to authorized parties who have a business need to know. Confidential information may be disclosed only within the college or to other parties in accordance with applicable law, confidentiality agreements, and privacy policies.

Sensitive Information (Data) handling

Sensitive information or data refers to confidential, privileged or proprietary information that is available to or readily accessible by the general public. If sensitive information is lost or used in any way other than intended, the result can be severe damage to the people or the institution to which that information belongs.

Common examples of sensitive information include:

- Personally Identifiable Information (PII): DOB, driver's license numbers, financial account information, medical records etc.
- All documents and emails marked "privileged and confidential", financial documents and account information.

All members with access to such sensitive data must adhere to the following best practices:

1. Do not communicate or otherwise transfer sensitive information to others unless you know they are approved or authorized to receive it;
2. Do not store unencrypted sensitive information on a laptop computer/desktop computer's hard drive, USB drive, CD, flash memory card, floppy drive, or other storage media. Do not store unencrypted sensitive information on any smartphone, tablet, or other mobile computing device;
3. Do not transmit sensitive information via any wireless technology, e-mail, or the Internet unless the connection is secure, or the information is encrypted;
4. Do not store sensitive information obtained from the College systems on third-party media or other systems unless doing so is specifically authorized by the College;
5. Dispose of media (such as disks, tapes, hard drives) that contain confidential information in a manner that protects the confidentiality of the information.

Reporting Security Incidents

Any member who believes that unauthorized use of the College information has occurred, should report it immediately to the head of IT. This helps to contain the incident and assists with managing its impact. Under certain circumstances, College may be required to notify others if sensitive information is compromised.

Violation of this entire policy can lead to reprimand, suspension or dismissal.