**2015-06-10** **No. MGMT-IST-00**

**Title: Dawson IT User Policy**

**CLASSIFICATION:** INFORMATION SYSTEMS & TECHNOLOGY
**FIRST ADOPTED:** (V1.0) May 13, 2009 by Management Group
**AMENDED:** (V1.1) April 27, 2011 by Management Group

## Goal

The goal of this policy is to ensure that the College's IT resources are used to support Dawson's Mission in the best possible way and to clearly define the standard of conduct expected from those making use of the College's IT resources. IT resources are intended to support the Mission of the College in all its aspects.

## Scope

This policy applies to all employees, students and other users of the College's IT resources.

The College's IT resources include the computers, peripherals, networks, software and computer-readable data either owned by the College or over which the College has jurisdiction, as well as the IT services that the College provides.

## Policy Statement

Users shall:

1. Use these resources in support of the College's Mission.
2. Use these resources in an effective, ethical, and lawful manner.
   a) Do not engage in forbidden activities including, but not limited to, cyber-harassment, hacking and spamming.
   b) Respect the copyright of the owners of software and data.
   c) Take no action which could compromise the integrity or normal operations of these resources.
3. Not use these resources for unauthorized commercial activities.
4. Use only resources for which they have authorization, and use them in the prescribed manner.
5. Not use their account to misrepresent themselves, others or Dawson College.
6. Not allow third parties to use their account and take reasonable measures to prevent such access.

## Application

The Director of Information Systems and Technology is responsible for the application of this policy.

Failure to meet its conditions may result in an investigation, which may lead to the suspension of an account. Where appropriate, the matter may be referred to those with the appropriate jurisdiction for further consideration and possible additional sanctions.

Accounts may be re-instated by the Director or designate, who may consult other Directors, or upon review and recommendation by the Director General.

## Review

The Director of Information Systems and Technology is responsible for the periodic review of this policy.

*Adopted by the Management Group on May 13, 2009*

*Revision adopted by the Management Group on April 27, 2011*