B5002 – COMPUTER AND COMPUTING SYSTEM USE

PROCEDURES

1. Users are responsible for all activities carried out through their user accounts, and are responsible for reporting any discovered unauthorized access or improper usage of the computing system.

2. Users will take precautions to secure and protect their user accounts, and are responsible for ensuring they have adequately complex and obscure passwords on College systems and devices. Users will change passwords annually or more frequently, and/or immediately upon request of the CIO or designate. Users will not share their account ID and/or password information with anyone.

3. When an investigation into an alleged breach is initiated, user access to the system may be revoked or suspended at the discretion of the CIO or designate, pending the outcome of the investigation. The affected user will receive notice of the investigation and revocation/suspension of access from the CIO or designate no later than two (2) business days after the revocation or suspension.

4. Users will respect the integrity of the computing system, and will not attempt to gain access to or alter any protected/shared resources without the approval of the CIO or designate.

5. Users bear the sole responsibility for the material they choose to access, send or display.

6. Users will follow instructions as posted or provided with respect to shared resources including, but not limited to, access to workstations, disk storage, internet resources, cloud computing systems and printing.

7. Users will not tamper with, open, or read other users' files, passwords and/or accounts. Users will not attempt to intercept or access data communications or data not intended for that user.

8. Users will not use the computing system to view or display sexually explicit material, obscene or lewd material, or material promoting hate towards individuals or groups based on colour, race, religion, gender identity, sexual orientation, and ethnic origin or place of origin, unless for academic purposes.

9. Users will comply with the licensing and copyright requirements of programs and data, including text, sound, images and other media.

10. No illegal copies of copyrighted or licensed software or other materials may be used or created.

11. Users will not physically attach any additional device (such as an external hard drive, printer or video system) to the computing system which might knowingly result in compromising the computing system in any way.

12. Users will use only computer software provided by the College. Personal software is not to be used on College computers, unless it has been legally acquired through licensing or other legal means and pre-approved by the IT department.

13. When using personal devices for academic or administrative purposes, it is the user's responsibility to ensure their devices are compatible with the College's systems, and to ensure that their devices are safe and protected from malware and viruses prior to each connection to College systems and networks.

14. It is the responsibility of the user to consult College-released materials regarding cyber security and information security threats (e.g. phishing attempts and ransomware), and adhere to recommended actions during those instances.

15. The IT department will provide the College community with notification of current cyber and information security threats.