B5002 – COMPUTER AND COMPUTING SYSTEM USE PROCEDURES

1. The CIO or designate is responsible for the development of College policy regarding the use of computing technology and systems.

2. The CIO or designate will authorize access to and use of the computing system.

3. 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.

4. Users and/or borrowers of IT equipment are responsible for the safekeeping and proper care of devices. The user in some cases may be liable for damages caused by unreasonable use, abuse, neglect, and alterations to equipment.

5. Users are expected to protect IT equipment from loss and damage and must immediately advise the IT Department if equipment is lost or stolen.

6. Staff in supervisory roles are responsible for the immediate return of IT equipment used by staff/direct reports who depart the organization. Unless otherwise arranged, Langara-provisioned equipment will be returned to the IT Department by the supervisor within 24 hours of staff termination/end date.

7. Users are responsible for ensuring they have adequately complex passwords on College systems and devices. The College adopts the BC government's current 14-character minimum standard for all passwords. Users are strongly encouraged to use passphrases that meet minimum complexity requirements, as they provide greater security and are more resistant to hacking attempts. Passwords must be changed annually or as security considerations dictate. Users must also update their passwords immediately upon request by the CIO or their designate.

8. The College does not support the use of third-party password managers (e.g., 1Password, LastPass, or Dashlane). Users should exercise caution when selecting a password manager because these vendors store personal information. Individuals who choose to use a password manager do so at their own risk.

9. Employees or students who discover a breach of their computer and/or computing systems will notify the IT department immediately. This includes physical security breaches, forced entry, and break-ins to classrooms, offices, labs, etc. where IT equipment is available for use.

10. Violations of the Computer and Computing System Use Policy may result in disciplinary actions including, but not limited to, suspension of the user from access to the computing system, prohibiting the user from further use of the computing system, suspending or expelling students, and reporting violations to law enforcement agencies and applying other College disciplinary procedures.

11. Access to the system can be removed during the investigation of a suspected compromised computer or account incident, whether by the action of a user intentionally or unintentionally triggering the incident.

12. 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.

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

14. Users will not engage in activities harmful to the computing system, such as creating or propagating viruses, disrupting services, damaging files, illegally downloading material, or intentionally damaging equipment, software or data belonging to the College. Users will not distribute forms of electronic communication that may cause excessive network traffic or computing loads, except as authorized.

15. Users will respect the rights and requirements of others entitled to use the computing system and refrain from overusing shared resources such as access to workstations, disk storage, Internet resources, cloud computing systems, and printing.

16. Students with disabilities will have the right to priority access at specially designed workstations. Other students may use those workstations only if there are no students with disabilities waiting.

17. Users will respect the privacy of others and will not tamper with, open, read, or share other users' files, passwords and/or accounts. Users will not attempt to intercept or access data communications or data not intended for that user.

18. Users will not conceal their identity or impersonate others when sending electronic communications.

19. 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.

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

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

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

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

24. USB flash drives and other secondary/portable hard drives pose a particular threat to the safety of the College network and potentially, the confidentiality of student/staff personal information. Secure remote access provisions and use of O365 repositories (e.g. SharePoint, OneDrive, Teams, as well as Workday) have been made to ensure staff and faculty have appropriate access to client data without resorting to unsecure/easily lost transport media such as USB drives. No staff or faculty shall use such secondary hard drives for transferring sensitive College data between Langara and other off-campus devices/repositories. Sensitive data includes, but is not limited to, class lists, staff/student personal information such as names, addresses, phone numbers, etc.

25. 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.