



## TECHNOLOGY GOVERNANCE POLICY

Approving Authority: Academic Coordinating Committee

Policy Owner: Vice President, Information Technology & Systems

Policy Lead: Manager, IT & Systems Budget, Assets & Reporting

Effective Date: 2024/11/20

Revision Date: N/A

### POLICY STATEMENT

The purpose of this policy is to outline technology governance at the Conestoga College Institute of Technology and Advanced Learning (Conestoga). Technology is intended to support Conestoga's Strategic Plan, mission, teaching and learning, and enhance its administrative, academic, and research functions. This policy is intended to inform technology users of the standard defined by Information Technology and Systems (IT and S) for use of technology at Conestoga, including resources, services, and infrastructure throughout its lifecycle.

### SCOPE

This policy applies to all technology users. This policy applies to all technology owned, leased or in the care, custody, or control of Conestoga at any of its campuses, offices, centers, sites, facilities, or locations where Conestoga business takes place. It also governs the selection, acquisition, usage, and decommission of all technology at Conestoga.

### DEFINITIONS

**Cellular Device:** Any electronic device that can connect to a cellular network using the mobile service provider's SIM card installed within it.

**Conestoga Business:** Activities performed for business and operations purposes on behalf of Conestoga including academic, administrative and research activities and purposes.

**Contractor:** Any person or entity contracted by Conestoga to provide goods or services on Conestoga-owned or leased property or at Conestoga coordinated off-site programs, functions, or events. A contractor shall be considered an employer and meet or exceed Conestoga's health and safety management system requirements unless otherwise determined to be a constructor.

**Data:** Individual symbols or pictures that represent raw facts or figures, which on their own do not comprise meaning and have no discernible arrangement. It can be processed by a computer, computer system or application.

**Employee:** An individual employed by the College, whether employed full-time, part-time, or on a contract basis, and includes, but is not limited to, faculty, researchers, support staff and administrators.

**Guest:** An individual who is not an employee, contractor, or student and is external to Conestoga, which includes, but is not limited to, Board members, visitors, alumni, and volunteers.

**Information:** Data that has been given value or meaning through interpretation or analysis and that has been organized to create meaning.

**Mobile Device:** Any communication device that does not require a physical wire to relay information from one device to another. It is designed or architected product that is able to be moved easily and used at a variety of locations.

**Multifactor Authentication (MFA):** Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric). MFA is generally considered secondary authentication in addition to a primary authentication method.

**Passphrase:** A secret consisting of a sequence of words or other characters to authenticate an identity or to authorize access to data. A passphrase is like a password in usage but is generally longer for added security.

**Password:** A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data.

**Student:** An individual enrolled in a course or courses at Conestoga, including full-time and part-time.

**Technology:** Any computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data or information. Components can include, but are not limited to, computers and associated peripheral devices, computer operating systems, utility/support software, accounts, and communications hardware and software.

**Technology Resource:** Any hardware, software, or communication equipment that a user interacts with for data or information management. This includes but is not limited to computers, mobile devices, cellular devices, applications, user accounts, wired and wireless network services that a user uses for tasks such as creating documents, sending messages, or retrieving data or information from repositories. These resources are owned, leased or in the care, custody, or control of Conestoga.

**Technology User:** An individual or entity that uses technological tools, devices, or systems for various information and data tasks, which includes, but is not limited to, guests, contractors, students, and employees. These users are authorized to use technology resources owned, leased or in the care, custody, or control of Conestoga with proper authentication and/or identification.

# **POLICY**

## **1. Technology Governance Mission Statement**

Conestoga is committed to providing technology that is safe and secure for all technology users. The provided technology will be scalable, robust, and modern to promote educational outcomes and goals. Technology will be provided that is human centric, community focused, sustainability driven, and in alignment with Conestoga's Strategic Plan, vision, mission, and values.

### **1.1. Safe and Secure**

Technology will be selected that is safe, securely designed, and kept up to date for technology users, and the organization. Harm caused by technology shall be analyzed, recorded, and appropriate harm reduction processes taken. Technology with undue harm levels will not be tolerated, and technology risks shall be assessed and managed to an acceptable risk tolerance level. The risks associated with technology at Conestoga will be mitigated by compliance with regulations, legislation, and guidance from relevant external bodies such as provincial and federal organizations.

### **1.2. Scalable, Robust, and Modern**

Technology will grow and contract with its usage while providing a stable, reliable, and acceptable technology user experience under all conditions of usage. Technology will be designed and deployed with overlapping levels of redundancy and resiliency with backup, recovery, and replacement in mind. Technology will be kept within supported life cycles and reviewed for replacement or upgrade on a standard cadence.

### **1.3. Education-focused**

Technology will be focused on the best education experience and outcomes for all technology users. Technology will support, enhance, improve, and drive Conestoga's mission and student success. Technology will be used to support learning goals in alignment with Conestoga's educational vision.

### **1.4. Community Focused and Human-Centric**

Technology will be designed and deployed for use by all technology users, considering the use of assistive devices, differences in technology interfaces, and adhering to all required regulatory and legislative requirements for access. Technology will not be selected for the sake of technology, but for the sake of technology users of said technology. Technology will be a bridge for all technology users to reach common ground and understanding while enhancing the College and wider community.

### **1.5. Sustainable**

Throughout the technology lifecycle, sustainability, reuse, reallocation, and recycling will be followed and promoted. Technology will be used and retained for as long as reasonably possible while providing the required outcomes. All technology will be acquired and disposed of in a manner that aligns with and promotes sustainability.

## 2. Technology Register

Conestoga will maintain a register of technology. This register will contain a listing of all technology that Conestoga has owned, leased or in the care, custody, or control of Conestoga with current licensing and support. The register will contain information about the intended audience, the technology type and intended usage, supporting documentation or training, and when the current supported technology may be reviewed, renewed, or removed. IT and S will be the responsible party for maintaining, updating, and modifying the register.

## 3. Monitoring and Auditing

Conestoga will monitor the usage and status of technology as part of ongoing operations. This monitoring will be for tracking issues, supporting technology users, and ensuring proper usage of technology. Technology monitoring will also include security monitoring to ensure that technology remains safe and secure. Technology auditing will be done on a regular basis to ensure proper access control, acceptable technology usage, and that technology is functional and is in a supported state.

## 4. Expectation of Privacy

Conestoga may access and use all information and data stored on and communicated through its technology resources for lawful purposes, including to facilitate work in an employee's absence, to conduct routine technical administration, to routinely audit system use, to investigate suspicions of improper use, any other misconduct, and to comply with legislation and regulations. Technology users who engage in personal use on technology resources are deemed to accept that Conestoga has the right to access and may raise no expectation of privacy that prevents Conestoga from accessing and using information and data for its intended purposes.

## 5. Violations

All technology users share responsibility for complying with and reporting violations of this policy. Violation of this policy may result in the suspension of privileges and/or other disciplinary action as warranted. Conestoga reserves the right to restrict any services or programs that are deemed to violate this policy. Conestoga reserves the right to recover its technology if direct or indirect costs are incurred because of any violation of this policy.

## 6. Accountability

- 6.1. Conestoga senior IT and S leadership, which is comprised of the Vice President, Directors, Associate Directors, and the Office of the Vice President, will be responsible for ensuring that all technology follows this policy.
- 6.2. IT and S department members are responsible for ensuring that they are knowledgeable of this policy and can apply it to their daily work.
- 6.3. Technology users are responsible for reading and understanding this policy.

## **RELEVANT LEGISLATION AND RELATED DOCUMENTS**

- The [Criminal Code](#) of Canada

- Canada's [Anti-Spam Legislation](#)
- Accessibility for Ontarians with Disabilities Act ([AODA](#))
- The Personal Information Protection and Electronic Documents Act ([PIPEDA](#))
- [Employment Standards Act](#)
- Freedom of Information and Protection of Privacy Act ([FIPPA](#))
- Acceptable Use of Technology Procedure
- Acceptable Password and Passphrase Procedure
- [Employee Code of Conduct Policy](#)
- Employee Discipline Procedure
- [Protection of Privacy Policy](#)
- [Applied Research Policy](#)
- [Social Media Guidelines for Conestoga Employees](#)
- [Student Rights and Responsibilities Policy](#)
- [Technology Lifecycle Management Policy](#)
- [Technology Asset Management Procedure](#)
- [Wireless and Mobile Device Technology Management Procedure](#)

## REVISION LOG

2024/03/13	1.0 draft created for policy review.
2024/11/20	Academic Coordinating Committee approval