ACCEPTABLE USE OF TECHNOLOGY PROCEDURE

Approved by: Academic Coordinating Committee

Authorizer: Chief Information Officer

Reference Code: IT2_V2

Effective Date: 9/28/2011

PROCEDURE STATEMENT:
This procedure outlines a basic framework for defining what is deemed to be acceptable and appropriate use of the Information Technology resources of the College. The use of Conestoga's Information Technology resources is a service extended to authorized users to support academic, research and administrative services, and it is Conestoga's expectation that these resources be used appropriately at all times.

All users of Conestoga's information technology resources must only use these resources for the purpose in which they are intended and respect the rights of other users, the integrity of the physical facilities and comply with all pertinent licenses and contractual agreements, as well as, applicable provincial and federal laws, regulations, policies and procedures. Conestoga's Information Technology resources remain the sole property of Conestoga.

SCOPE:
This procedure applies to all members of the Conestoga Community using, accessing or handling Conestoga's Information Technology resources at any of its campuses, offices, centres, sites and/or facilities.

DEFINITIONS:
Conestoga Community refers to all registered students, both full-time and part-time; all employees, full-time, part-time and casual; all others associated with Conestoga including board members, retirees, alumni or volunteers, and visitors who are granted temporary permission to use Conestoga's Information Technology resources.

Academic, Research and Administrative services refers to the business and operations of the college to provide teaching and learning in the delivery of higher education.

Information Technology (IT) resources are services, facilities, and equipment including, but not limited to: computer systems; networks; data storage media and content/data; software applications; hardware or; any other electronic, telecommunications or portable device used for the digital transmission of information, on campus or remotely, through which Conestoga provides access or is connected.

Portable devices include, but are not limited to, laptops, notebooks, PDA's, USB keys, mobile devices (e.g. cellular phones, smartphones), and external digital storage devices.

Personal Information as defined in the Freedom of Information and Protection of Privacy Act, R.S.O. 1990, refers to any recorded information about an identifiable individual, including,

a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

c) any identifying number, symbol or other particular assigned to the individual,

d) the address, telephone number, fingerprints or blood type of the individual,

e) the personal opinions or views of the individual except where they relate to another individual,

f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

g) the views or opinions of another individual about the individual, and

h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

Confidential Information refers to any information received in confidence that is not to be disclosed or made use of for any purpose other than that for which it was intended.

Social media are defined as media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Examples include but are not limited to LinkedIn, Twitter, Facebook and YouTube.

Malware refers to malicious software, the intent of which is to disrupt or breach security measures, gather personal information or engage in any other type of abusive behavior. This includes, but is not limited to computer viruses, worms, trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, and other malicious and unwanted software or program.

Unauthorized access (hacking/spoofing/phishing/hijacking) may include the use of, or attempted use, of unauthorized user names, passwords, computer addresses or identities, or modifying assigned network settings to gain access to computer/telecommunication resources and/or data and telephone records, or otherwise attempting to evade, disable or "crack" Conestoga's security provisions or external systems.

GUIDING PRINCIPLES AND REGULATIONS:

System/network security

Users must respect and abide by all security measures that have been put into place. Unauthorized or deliberate attempts to bypass or alter security measures are considered violations of this policy/procedure.
Hacking, or any other action by any individual to subvert or disrupt the intended functioning of any facility is strictly prohibited. No person(s) shall by any wilful or deliberate act, jeopardize the integrity of the computing equipment, its systems programs or other stored information.
Users must not disconnect computer equipment cables, remove batteries from remote control devices or in any way alter any equipment/resources in classrooms or offices.
Unless authorized by Conestoga, technology resources must not be used for commercial purposes. This includes, but is not limited to, selling products or services for personal gain or profit, distributing advertising materials, offering network information or services for sale, and/or operating a personal business or comparable venture.
Members of the Conestoga Community are not allowed to give, sell, or otherwise provide computing resources to individuals or groups that do not have explicit permission, from Conestoga, to use them. Conestoga retains the exclusive right to grant and revoke access to Information Technology resources.

Network disk space

Data storage resources are shared Conestoga resources the usage of which is controlled and monitored to ensure legal, fair and reasonable access for all of the members of the Conestoga Community. This resource is finite in nature and all users share the responsibility of ensuring that these resources are not squandered or misused. Conestoga does not provide any expressed guarantee or assurance over the privacy of information on these resources, and reserves the right to access and manage all stored information on or transmitted within the Conestoga computing infrastructure. All information stored within Conestoga's computing infrastructure, including information in individual accounts and e-mail, is the property of the Institution. All information stored on the Conestoga infrastructure must exclusively exist to support a specific administrative, academic or enterprise requirement and/or need.

Personal and/or confidential information

Every employee bears the primary responsibility for the information that they collect, send, access, or view. Employees should refrain from copying and/or transporting information of a personal or sensitive nature on portable storage devices. If this cannot be avoided, then it is the responsibility of the user to ensure that any personal or confidential information stored on a

portable device de-identifies personal information, is encrypted and secure at all times. The user is also responsible for ensuring that any copied data on a portable device is deleted or erased appropriately, as soon as it is no longer needed.
Use of personal or confidential information in violation of the Freedom of Information and Protection of Privacy Act is strictly prohibited and will result in disciplinary action.
Any user processing payments on behalf of Conestoga must adhere to the conditions outlined in the Conestoga PCI procedure document.

Social Media
Conestoga is committed to utilizing social media to enhance its profile and reputation, to listen and respond to student opinions and feedback, and to drive enrolment, loyalty and advocacy. All social media content posted on behalf of Conestoga must be approved by the Marketing and Communication department. Employees are responsible for ensuring that anything they post to social media sites is appropriate, respectful, accurate, and not in violation of this or any other Conestoga policy. Conestoga reserves the right to request that certain subjects be avoided, withdraw certain posts, and remove inappropriate comments and content. Any statement by an employee of the college, in reference to the college must be in accordance with the employee's employment at the college. More information is provided in the Social Media Guidelines for Conestoga Employees.

User ID and Material
Each User is solely responsible for managing the User ID that they have been assigned by Conestoga to gain access to the available Information Technology resources. Users must not allow any other person to use their user ID, and will be held responsible for any violations of this policy/procedure that are associated with their user ID. Passwords should be kept secret and never given to anyone else. Users shall not attempt to obtain a User ID under false pretences or forge/attempt to forge electronic mail messages.
Under no circumstance may a User access, inspect, alter, delete, publish or otherwise tamper with files or file structures (including documents such as email messages) that do not belong to the User without prior consent or authorization for such activity with respect to such files or file structures.
Users of Conestoga's Network are fully responsible for any material or information that they post, input, upload, download, access, provide, submit or transmit through email, the World Wide Web or in any other manner. Users must ensure that they have all necessary rights and licences to such information. Users must not breach copyright by installing, reproducing and/or distributing copyrighted materials such as proprietary software, publications or files without permission. Conestoga software is provided under licence agreements with various vendors and may not be copied or otherwise removed.

Correspondence and Messaging
Conestoga correspondence should only be disseminated electronically through the official Conestoga-provided e-mail, and in accordance to the E-mail, Voice mail and Corporate Calendar Guidelines. Electronic messages sent by Conestoga employees must conform to Canada's Anti-Spam Legislation (CASL). Express or implied consent of all intended recipients is required for the dissemination of any commercial electronic messages. All such messages must also contain

information about the sender as well as an unsubscribe mechanism. More information and guidance on CASL and its implications for Conestoga is provided in the Employee section of the Conestoga website.

Respect of others

Users are expected to be respectful and polite by:

- monitoring noise levels; users seeking to access audio content should use headphones. Users are solely responsible for providing their own appropriate and acceptable headphones.
- keeping clutter to a minimum;
- keeping food and beverages away from computer systems and other electronic resources
- refraining from displaying images or texts which are inappropriate

All users have a right to work and study in an environment free from discrimination/ harassment. Any materials of a harassing or defamatory nature which may violate these rights are not to be stored, displayed, transmitted, posted to news groups or otherwise linked to Information Technology resources.

Any process that causes a user to be deprived of services or resources that they would normally expect to have available is not allowed. This covers but is not limited to the creation of "Spam," playing computer games, downloading of audio and video files, introducing malware (viruses, worms, etc.) or creating/circulating electronic chain letters.

Further, Conestoga resources must not be used to harass other users with inappropriate messages, copy/steal the intellectual property of others, or engage in any other behaviour which violates their intended use.

Conestoga fully endorses and supports the individual's right of expression and will not act as a censor. However, accessing or displaying pornographic, obscene, debasing, sexually explicit, racist, defamatory or violent images and/or initiating unsolicited communication of this nature is generally prohibited. Special considerations and exceptions may be granted to support specific/demonstrable academic purposes or objectives. In such cases users and faculty are encouraged to contact the Directors of Information Technology and Information Management Systems (formerly Computer Systems) and seek advice and/or approval in advance. Conestoga is obligated to investigate all reported complaints to ensure compliance with this policy/procedure, applicable federal and provincial laws and with other Conestoga policies and procedures. The presence of information that may offend, upset or otherwise be deemed unacceptable by users in no way represents any type of endorsement or sponsorship by Conestoga.

Software installation

User installation of software on Conestoga-maintained servers and hard drives is forbidden. This is to ensure compliance with software licensing and registration requirements and to protect against the proliferation of malware (viruses, worms, etc.). Unlicensed or unauthorized software found on Conestoga systems is subject to immediate removal. Pirated software will be removed from any machine on which it is found. No support for installation or use can be provided by IT Services for unauthorized software.

Games
Playing computer games on Conestoga resources is expressly forbidden, unless it is directly related to a program or course endorsed and approved by Conestoga.

Open Access Labs
Open Access Labs/Computers are available to students to access e-mail and the Internet and use installed software to increase their computer knowledge, enhance their computing skills and further their learning experience. The computers in the labs provide students with the latest in hardware, operating/applications software and related services. Users are expected to be considerate and respectful of other users.
Normal hours of operation for these computer labs are outlined in the Lab Policy. For security and safety reasons, not all computer labs will be unlocked during these times. If required, contact Security Services for access to a locked computer lab. You may be directed to use a lab that is already unlocked if the resources (software) you require are available. Lab access can be extended by contacting your program coordinator.
Under no circumstances should computers, printers, cabling or other peripheral equipment associated with the computer lab be moved, modified or disconnected.
Network printers and associated supplies (toner cartridges and paper) in the computer labs are paid for from the student technology fee. Please avoid printing multiple versions of documents by proofreading and correcting the materials on-screen. For further information please refer to the Student Printing Guidelines document.

Examples: <u>Unacceptable</u> Use
The following list contains a few examples of unacceptable use of Information Technology resources. If an activity is suspected as being unacceptable, it should be reported to the IT Service Desk and/or Directors of Information Technology Services and Information Management Systems (formerly Computer Systems).

- Using another individual's account access
- Granting another individual access to your account
- Sending messages deemed as discriminatory, obscene, abusive, derogatory or harassing
- Displaying, transmitting, distributing or making available information that is or may be perceived as discriminatory or implies/intends to be discriminatory
- Using Conestoga's computer resources for any purpose that violates the Criminal Code of Canada
- Creating, posting, forwarding, etc. information that may contravene the Ontario Human Rights Code or Criminal Code of Canada
- Using Information Technology resources to interfere with or disrupt the network for other Users
- Using resources for political or commercial reasons
- Entering facilities, using equipment, software resources or accounts without authorization
- Intentionally sending computer worms, viruses or other disruptive materials

- Creating and/or using world-wide web information pages or links to point to offending materials that do not comply with the Ontario Human Rights Code or the Criminal Code of Canada;
- Using a resource for purposes other than those that it was intended to be used for.

RESPONSIBILITIES:

All Conestoga Community users are expected to abide by the Acceptable Use Policy and Procedure, and are accountable for their actions. Supervisors are responsible for monitoring compliance within their jurisdictions. Users are also expected to comply with the directions given to them by staff when performing their regular or delegated duties regarding this policy/procedure.

Employees, students and clients are responsible for reporting all real, or perceived infractions of this policy/procedure to the IT Service Desk and/or Directors of Information Technology Services and Information Management Systems (formerly Computer Systems).

The Information Technology department is responsible for:

- purchasing/maintaining/ revising/upgrading IT services, facilities and equipment;
- regularly communicating changes to processes
- monitoring IT usage
- investigating infractions

PROCEDURE:

All reasonable attempts have been made to ensure the privacy of user accounts, electronic mail and telephone accounts established for students and employees.
Conestoga reserves the right to access all email, including data in transit and stored telephone records and all information stored on the network. Employees and Students should not use Conestoga technology resources for personal use.
If an infraction to this policy/procedure is suspected, Conestoga will exercise its right and authority to conduct appropriate search procedures of all Conestoga owned and operated information technology resources. Unless an infraction poses an immediate threat to Conestoga, approval is required prior to commencing any search procedure. Conestoga reserves the right to review and/or restrict any services and programs that are deemed to violate any of its policies.
If a policy/procedure violation is discovered it must be reported immediately. Failure to adhere to this policy/procedure may result in suspension of user privileges, and/or other disciplinary and legal action, as appropriate, including but not limited to, the remedies outlined in the Student Code of Conduct Policy and/or Employee Code of Conduct Policy and/or Discipline of Employees Policy.

Reporting an Alleged Violation

1. Employees are responsible for reporting violations and/or suspected violations of the Authorized Use of Information Technology to their immediate supervisor. Students and

clients are responsible for reporting violations and/or suspected violations of the Authorized Use of Information Technology to the IT Service Desk and/or Directors of Information Technology Services and Information Management Systems (formerly Computer Systems).

2. The Information Technology department will conduct a preliminary investigation of the violation or incident. An assessment report outlining the seriousness and scope of the violation, plus the specific policies and laws that were breached will be created and sent to the Directors of Information Technology Services and Information Management Systems (formerly Computer Systems) for further review.

3. Minor infractions will result in a verbal warning by the appropriate authority. A copy of the incident report will be placed in the student or employee file.

4. Infractions of a more serious nature will be reviewed more thoroughly and adhere to standard investigative protocols and methodologies.

Disciplinary Action

On any violation of policy, Conestoga will exercise its right to take appropriate disciplinary actions and/or sanctions. These may include but not be limited to the following:

- Verbal/written warning
- Rescinding of access to resources
- Removal of materials
- Disciplinary directives
- Behavioral contracts
- Suspension from Conestoga
- Expulsion/dismissal from Conestoga

Conestoga is obligated to report all violations of law to appropriate authorities. Conestoga is not responsible for any actions and/or sanctions taken by these authorities.

DISCLAIMER:

Conestoga accepts no responsibility for any damage or loss, due directly or indirectly, to the use of its Information Technology resources. It makes no representation of warranty, expressed or implied, regarding the computing resources offered, or their fitness for any particular use or purpose. This Policy/Procedure is not a complete statement of Conestoga's rights or remedies, and nothing in this Policy/Procedure waives any of those rights or remedies.

REFERENCES:

- Acceptable Use of Technology Policy
- Student Code of Conduct Policy
- Employee Code of Conduct Policy
- Protection of Human Rights Policy/Procedure
- Email, Voicemail and Corporate Calendar Policy
- Electronic Communication Policy for Students
- Social Media Guidelines for Conestoga Employees
- Discipline of Employees Policy/Procedure
- Criminal Code
- Additional Federal/Provincial legislation
- Conestoga PCI Procedure
- Lab Policy
- Conflict of Interest/Use of College Resources Policy
- Conflict of Interest/Use of College Resources Procedure

REVISION LOG:

- 2011-07-15, Minor title reference updates
- 2011-08-16, Policy and Procedure Committee - reviewed
- 2011-09-27, Policy and Procedure Committee - approved
- 2011-09-28, Academic Coordinating Committee – approved
- 2014-06-25, Update of formatting to meet AODA requirements
- 2014-07-22, Update to Guiding Principles and Regulations and References sections to refer to new CASL requirements
- 2014-08-14, IT Strategic Steering Committee – reviewed
- 2014-09-15 Policy and Procedure Committee – approved
- 2014-09-24 Academic Coordinating Committee - approved