CONESTOGA VALLEY SCHOOL DISTRICT
2110 Horseshoe Road
Lancaster, PA 17601

School Board Policy

Policy Number: 239 **Section: Students**

Title: Acceptable Use Policy – Students

Related Policy: CV 239.1 Student Personal Electronic Devices

Date 1st Reading: January 18, 2011
Meet & Discuss: January 10, 2011
Approved: February 22, 2011
Date Revised:

239.100 Introduction and Overview Access to information technologies is integral to the educational mission and purpose of Conestoga Valley School District. The district utilizes technology to facilitate student instruction, district-sponsored activities, district services, research, and district operations. The purpose of this policy is to ensure district technology is used for its intended purposes; to protect the integrity of the district computer network, district technology and electronic data and to prohibit activities that undermine or are inconsistent with the intended use of technology within the district setting. This policy sets forth the district's expectations for its students who use district technology, as well as the use of personal technology by both students and other individuals while on district property or accessing the district's computer network. Because the district's use of technology is constantly changing, it is imperative that all students understand that the district's Acceptable Use Policy will be interpreted in a manner to fulfill the stated purpose of the policy. The district expects all students to utilize their best judgment when it comes to the use of district technology and keep in mind that this policy does not supersede other district policies, but rather addresses the appropriate use of both technology provided by the district and personally owned technological devices by students, but also community members, vendors and guests that use district and/or personal technology. **239.110 Introduction** 239.111 Supervision and Personal Responsibility All students utilizing district technology are also subject to the terms and conditions of this Acceptable Use of Technology Policy. All students and their parents/guardians must sign an agreement stating that they have read and agree to the terms and conditions in this policy before they are given access to any district technologies. This permission form must be signed when the student is enrolled in the district or when they change buildings within the district.	Cites relating to	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34

Students may use the district technology in their regular courses and student activities in compliance with this policy. The failure to comply with the terms of this policy may result in the temporary and/or permanent revocation of technology privileges and other forms of disciplinary action deemed warranted by the district.

The district provides sufficient information technology resources for each student for regular academic pursuits. If a particular project requires additional resources, the information technology department may work with students on a case by case basis to provide additional resources.

Students are not authorized to allow another individual (i.e., family member, other students) to use district technology resources entrusted to them for any reason, unless prior approval is obtained from the Manager of Computer Services.

239.120 Privacy
The district reserves the right to monitor and track all behaviors and interactions that take place online or through the use of district technology. Therefore, students have no expectation of privacy while using district technology on or off district property. The district also reserves the right to investigate any reports of inappropriate actions involving or relating to the use of district technology or personal technology that is used while on district property.

All emails and messages sent through the district's network or accessed on a district computer may be inspected at anytime for any reason. Any files saved onto a district technology or the district's network may also be inspected. Students have a limited expectation of privacy when using their own technology on district property or at district events so long as no activity violates policy, law and/or compromises the safety and well-being of the school community.

239.130 Filtering
The district adheres to the requirements set forth by the federal Children's Internet Protection Act (CIPA) and Pennsylvania's Child Internet Protection Act. This means that all district-provided access to the internet is filtered and monitored. The district cannot monitor every user's internet activity at all time, but it retains the right to monitor such user activities that via district technology. By filtering internet access, the district intends to block pornographic, offensive, obscene, and inappropriate images and content, which undermines and is otherwise inconsistent with the district's educational mission.

239.140 Right to Update
Since technology is continually changing, the district reserves the right to change, update, and edit this policy at any time in order to continually protect the safety and well-being of the district's community. Additionally, the district may establish additional rules, issue administrative directives and/or guidelines to fulfill the purposes of this policy.

239.150 Termination of Accounts and Access
Upon termination of official status as an a student with the school district, students will no longer have access to the district network, files stored on the district network, or district-provided email accounts. The district strongly recommends that students save their own purely personal data on their own personnel technology throughout their enrollment.

239.200 Definitions and Terms Section
"Bandwidth," "Cyber-Harassment,", "Internet," " Network," "Technology," "District Technology," "User," and "PDA"

239.210 Bandwidth
Bandwidth is a measure of the amount of data that can be transmitted in a fixed amount of time.

239.220 Cyber-Harassment
Cyber-harassment means the sending of electronic messages, pictures or other conduct using technology that denigrates or shows hostility or aversion towards an individual because of that individual's race, color, national origin, gender, disability or age that has the purpose or effect of substantially interfering with the individual's academic or professional development or creates an intimidating, hostile or offensive education or employment environment.

239.230 Internet
Internet is the international network of computer systems.

239.240 Network
The Network means the district-owned or operated computers, and electronic devices and other technology, such as printers, fax machines, scanners, etc. that are connected to each other for the purpose of communications, document/file creation, data storage and sharing and internet access for the benefit of the district.

239.250 Technology
Technology is a comprehensive term including, but not limited to, all computers, projectors, televisions, DVD players, stereo or sound systems, digital media players, gaming consoles, gaming devices, cell phones, personal digital assistants, CEDs, DVDs, camcorders, calculators, scanners, printers, cameras, external and/or portable hard drives, modems, Ethernet cables, servers, wireless cards, routers and the Internet.

239.260 District Technology
District technology means all technology owned and/or operated by the district, including technology temporarily or permanently issued to a student that may be used off district property.

239.270 User
User is an inclusive term meaning anyone who utilizes or attempts to utilize, whether by hardware and/or software, district technology while on or off district property. The term includes district students parents and/or guardians, and any visitors to the campus that may use district technology.

239.280 Personally Owned Device User
Personally owned device user refers to anyone who utilizes their own technology on property owned or controlled by the district or at a district-sponsored event.

239.290 PDA
PDA stands for personal digital assistant which is an electronic device which provides some of the functions of a computer, a cell phone, a music player, or a camera.

239.300 Acceptable Uses Section
239.310 User Orientation
All students must sign a statement about acceptable and unacceptable behaviors related to technology before they can utilize any district technology at the beginning of each school year.

239.320 Purposes and Use Expectations for Technology
The use of all district technology, including the district network and its Internet connection is limited to educational purposes and minimal incidental use. Educational purposes include classroom activities, career development, exploring post-secondary educational opportunities, and limited high quality educational activities. Commercial and recreational use of district technology resources is prohibited.

Students may not utilize district technology for the following reasons:

- to sell, purchase, or barter any items or services.
- may not share or sell their network resources to others, including, but not limited to, disk storage space.
- to access social networking, gaming, or other web sites for non-educational purposes.to access websites that contain sexually explicit content; promote or glorify activity that violates state or federal law or district policies.
- send or receive emails, instant messages or other electronic communications that contain sexual innuendo or sexually explicit conduct.
- to engage in personal conduct that has the purpose or effect of substantially interfering with a student's educational environment or a school employee's work environment or is inconsistent with the district's reasonable expectations for students workplace conduct.

239.330 Personal Responsibility
The district expects its students to act responsibly and thoughtfully when it comes to using technology. Students bear the burden of responsibility to inquire with the IT Department or district administrators when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

239.340 District Provided Technology Resources
Network storage is a finite district resource and we expect students to be respectful of other users and limit the amount of space and memory taken up on district computers and on the district network.

All students may be provided with a district email account for school-related communications. All emails sent from this account are representative of the district and students must comply with district policies and expectations regarding appropriate language and content of emails when sending and receiving them. Abusing these resources can result in the loss of this privilege. The district has wireless Internet that has security protection enabled. Permission must be obtained from the Manager of Computer Services in the Technology Department to connect personal laptops or hand held devices to the Internet.

Only Technology Department personnel or persons designated to do so may connect computers and devices to the district's Ethernet ports and/or disconnect computers and devices currently connected to the district's network.

Users will follow guidelines provided by the technology department to assure that access to district technology is protected by proper account authentication (e.g., password security and syntax requirements). Methods used may include that all students would change their passwords every 30 days; use passwords that are a minimum length of eight characters and include alpha, numeric and special characters; maintain a password history (i.e., approximately 10 passwords before a repeat); to lock out users after 3 unsuccessful attempts and to log off the system after a period of inactivity (i.e., 60 minutes maximum). Also, 18 character phrasing may be used which is superior to the above.

239.400 Unacceptable Uses of Technology Section

239.410 Cell Phones and PDAs

Cell phones and PDAs are permitted on campus, but are not to be used during the school day by students without prior authorization and in compliance with Policy 239.1. .

Students are only permitted to access facets of the district network that they have authorization for with their phones, PDAs or other similar devices and only for school district purposes.

Students are not permitted to create, display or transmit inappropriate content as defined by the Children's Internet Protection Act on their phones, PDAs or other similar devices while on district property.

Pagers are permitted on campus for students serving in volunteer fire or ambulance companies, but should not interrupt classes, work or other district activities.

239.420 Recording, Video, and Photography

Web cams may not be installed onto district computers. The installation of webcams on district computers shall only be done by district computer services personnel.

District-owned laptops with built in cameras and/or web cams may be used for educational activities, if the proposed use is approved by an instructional employee the building principal.

Webcams on personal computers shall not be used on district property, unless their use is for educational activities and approved by the students teacher and building principal.

239.430 Social Networking and Website Usage
While the district respects the rights of its students to establish and use social network profiles or accounts (i.e.: Facebook.com, MySpace, com, etc.), outside of school, these social networking websites should not be accessed using district's technology or while at school. Students using social networking website shall do so outside of school on their own personal technology devices and should not have content on their website that would material disrupt the educational environment.

Students may not access their electronic photography through websites such as Photo Bucket, Webshots, or Flickr, from district technology, unless such access is approved by the student's teacher as part of a course project.

Students are not permitted to use the district's technology to access any rating or dating websites including, but not limited to: Match.com, eHarmony, JDate, Black Planet, Hot or Not, RateMyTeacher.com, RateMyCoach.com, or Juicy Campus.com.

Do not access material that is offensive, profane, or obscene, including pornography and hate literature. Hate literature is anything written with the intention to degrade, intimidate, incite violence, or incite prejudicial action against an individual or a group based on race, ethnicity, nationality, gender, gender identity, age, religion, sexual orientation, disability, language, political views, socioeconomic class, occupation, or appearance (such as height, weight, and hair color).

239.440 Communication: Instant Messaging, Email, Posting, Blogs
Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students while using district technology. Inappropriate communication includes, but is not limited to the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by others ; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property including the acquisition or creation of weapons or other destructive devices. If you are told by another person to stop sending communications, you must stop. Communication with others should be of a respectful nature only and should relate to school academics or school events.

Do not post or send chain letters or spam. Spamming is sending an unnecessary and unsolicited message to a large group of people. Spamming can occur through emails, instant messages, or text messages.

239.450 Intellectual Property, Academy Honesty, Personal Integrity and Plagiarism

Students shall not claim or imply that someone else's work, image, text, music, or video is their own. This is plagiarism and will not be tolerated. Plagiarism is also when a piece of someone else's work is incorporated into students work without giving appropriate credit. All students are expected to maintain academic honesty. Students should not pretend to be someone else online or use someone else's identity without express permission from that person and/or his/her parent/guardian if he/she is a minor. Students may not use, post or make accessible to others the intellectual property; including, but not limited to text, photographs, and video; of someone other than themselves. This includes intellectual property that students were given permission to use personally, but not publically. This behavior violates district policy as well as state and federal laws.

A work or item is copyrighted when, among other issues, one person or one group owns the exclusive right to reproduce the work or item. Songs, videos, pictures, images, and documents can all be copyrighted. Copyright infringement is when you violate copyright law and use or reproduce something without the authority to do so. Students should appropriately cite all materials used in their work. Students should not utilize someone else's work without proper permission. Additionally, the schools' computers also have software on them that is protected by copyright law. This software is to be used only in the manner in which the school has the license to use it.

239.460 Gaming Devices

Students may not bring personal video game systems onto campus unless permission is obtained from the building administrators. These devices may only be turned on and played during non-school hours. Students may not use school technology to access, download or play non-educational computer games.

239.470 Downloads and File Sharing

Students may never download, add, or install new programs, software, or hardware onto school technology. Downloading sound and video files for personal use or entertainment onto school-owned computers is also prohibited. This prohibition applies even if the download is saved to a removable hard drive, CD or DVD.

Students may never configure school computers (or personally owned computer while on district property) to engage in illegal file sharing (i.e.: Kazaa, Napster or Limewire). The district will cooperate fully with the appropriate authorities should illegal behavior be conducted by students.

The likelihood of accidentally downloading a virus or spyware when downloading music and movies is very high; therefore, students may not download any sound or video files onto their personally-owned technological devices through the school's technology. Students also should not download any files or attachments from unknown senders.

239.480 Commercial and Political Use
Commercial use of district technology is prohibited. Students may not use district technology to sell, purchase, or barter any item or service Students may not transfer, share or resell their network resources to others, including, but not limited to, disk storage space. The district is not responsible for any damages, injuries, and/or claims resulting from violations of responsible use of technology.

Political use of district technology is prohibited. Students may not use district technology to campaign for/against, fundraise for, endorse, support, criticize or otherwise be involved with political candidates, campaigns or causes unless such activity is part of an academic course.

239.490 Respect for the Privacy of Others and Personal Safety
The district expects students to respect the privacy of others when using district technology. Students are prohibited from seeking information on, obtaining copies of, or modifying files and other data, using district technology. Students are prohibited from using the passwords belonging to others to gain access to electronic information accessing.

When using district technology, students may not: (1) misrepresent or assume the identity of others; (2) distribute or forward information that was sent to you privately without the permission of the person who sent you the information; (3) post private or confidential information about another person; (4) use another person's account.

The district prides itself on its reputation for excellence; therefore, employee student may not use the name, logo, mascot or other likeness or representation of a district school on a non-school website without express permission from the School Board. This includes pictures of anyone wearing clothes with the name, crest, emblem, or logo of the district or district school.

239.4100 Computer Settings and Computer Labs
Students are only allowed to alter, change, modify, repair, or reconfigure settings on district technology. This includes deleting cookies and history and falsely re-setting the time and/or date on the computer.

Purposefully spreading or facilitating the spread of a computer virus or other harmful computer program is prohibited.

Students may not circumvent any system security measures. The use of websites to tunnel around firewalls and filtering software is expressly prohibited. The use of websites to anonymize the user is also prohibited. The use of websites, both domestic and international, to circumvent any district policy is prohibited. Students may not alter the settings on a computer in such a way that the virus protection software would be disabled. Students should not attempt to guess passwords. Students may not simultaneously log in to more than one computer with one account unless required to do so as part of a job function. Students are not to access any secured files, resources, teacher, or administrative areas of the district network

No policy can detail all possible examples of unacceptable behavior related to technology use. District technology users are expected to understand that the same rules, guidelines and policies that apply to non-technology related student behavior also apply to technology-related student behavior. District technology users are expected to use their best judgment when it comes to making decisions related to the use of all technology and the Internet. Students should consult their teachers or the Technology Department for assistance if there are questionable issues.

239.500Consequences for Inappropriate Use of District Technology

The district provides its student with access to district technology in order to enhance their education. Student access to these resources is a privilege, not a right. The district reserves the right to restrict, suspend or otherwise terminate a student's access to district technology as deemed warranted.

Violations of this policy may result in the temporary or permanent revocation of a student's access right to district technology. Additionally, a student may be subject to other forms of disciplinary action for violations of this policy. The district will cooperate fully with local, state, and/or federal officials in any investigations related to illegal activities conducted using district technology. If a student accidentally accesses inappropriate information or if someone sends a student inappropriate information, the student should immediately tell a teacher or a member of the Technology Department so as to document that you did not deliberately access the inappropriate information.

If e student witnesses someone else deliberately accessing inappropriate information or use technology in a way that violates this policy, the student is required to report the incident to a teacher as soon as possible. Failure to do so could result in disciplinary action.

The district retains the right to suspend service, accounts, and access to data, including student files and any other stored data, without notice to the student if it is deemed that a threat exists to the integrity of the district network or other safety concerns of the district. The district reserves the right to confiscate personally-owned technological devices that create a threat to the integrity of the district network or other safety concern of the district.

239.600 District Liability

The district makes no warranties of any kind, either express or implied, in connection with its provision of, access to, or use of the district computer network and/or district technology. The district will not be responsible for any claim, loss, damages or costs of any kind suffered by, directly or indirectly, students or other individuals arising from a user's use of district technology of district computer network. The district is not responsible for any loss of data or interruption of service.

The district is not responsible for ensuring the acceptability, accuracy or quality of the information obtained through district technology, and the access to the same does not imply the district's endorsement of such content.

CONESTOGA VALLEY SCHOOL DISTRICT

STUDENT NETWORK ACCEPTABLE USE AGREEMENT

I have received and reviewed a copy of the **Conestoga Valley School District – Policy 239 Acceptable Use Policy for Students and Policy 239.1 Student Personal Electronic Devices**, which governs students' use of electronic devices while at school and when working with district owned devices. I understand that failure to follow the aforementioned policy may result in disciplinary action, such as, but not limited to, my access privileges being revoked or limited and/or appropriate legal action taken.

Name of Student (print): _____

Student Signature: _____ Date: _____

Signature of Parent/Guardian: _____ Date: _____