NEW CASTLE COUNTY
VOCATIONAL-TECHNICAL SCHOOL DISTRICT
BOARD OF EDUCATION

Section:	600
Title:	Acceptable Use Policy
Policy #:	608
Adopted:	7/28/10
Revised:	4/23/2012

ACCEPTABLE USE POLICY

1. Purpose

The purpose of this policy is to establish acceptable and unacceptable use of the Covered Electronic Resources provided by New Castle County Vocational Technical School District ("NCCVT"), and the State of Delaware (collectively with NCCVT, the "District"), to Covered Users. Covered Electronic Resources are provided for a limited education purpose for students and to facilitate employees' work productivity. This policy serves to ensure that actual use conforms to this intended purpose.

This Policy is intended to supplement other District policies, including the District's policy on Confidentiality, Anti-Harassment, etc.

Any questions about this Policy should be directed to the Supervisor of Technology.

2. Scope

a. Covered Technology

This policy applies to "Electronic Resources," which are those resources that are: (a) provided by the District; (b) paid for, in whole or in part, by the District; (c) used to conduct business or other activity for or on behalf of the District; or (d) used in or at a District facility. Covered Electronic Resources include, without limitation, the following:

- "E-mail", which includes to all electronic-mail accounts and services provided to Covered Users by the State of Delaware or NCCVT;
- "Computer Resources", which includes all computers and related resources whether stationary or portable, including but not limited to all related peripherals, components, disk space, storage devices, servers, and output devices such as telephones, hand-held devices, printers, scanners, and copiers, whether owned or leased by the District;
- "NCCVT Network", which includes the infrastructure used to transmit, store, and review data over an electronic medium, and includes any and all of the following technologies provided to authorized users: (a) Internet service; (b) intranet system; (c) NCCVT mainframe system; and (d) any collaboration systems, including but not limited to calendaring, message boards, conference boards, blogs, text messaging, instant messaging, video conferencing, websites, and podcasting, whether the system is owned or contracted;
- "Electronic Data", which includes any and all information, data, and material, accessed or posted through any Electronic Resource; and
- "Personal Communication Devices", which includes any cellular phone, smartphone, personal digital assistant, or other personal electronic communication device.

b. Covered Users

This policy applies to all "Covered Users", which includes:

- Employees, contractors, consultants, temporary, and other workers at the District, including all personnel affiliated with third parties;
- NCCVT board members and officers;
- Volunteers and interns performing work for or otherwise acting on behalf of the District; and
- NCCVT students.

3. General Guidelines for Use

The following guidelines summarize the principles underlying this policy and serve as an effective baseline for evaluating whether a particular use violates those principles.

- Electronic Resources are not intended for public access. The District has the right to place reasonable restrictions on the use of Electronic Resources.
- Users are required to observe all rules and obligations set forth elsewhere by the District (for example, in the Board of Education Policy Manual or Student-Parent Handbook) or by law at all times. This policy is intended to supplement, not replace, those duties.

- Access to and use of Electronic Resources is a privilege, not a right. Parent or guardian permission is required for all students under age 18.
- As set forth in more detail in Section 7, below, the District reserves the right to monitor any and all use of Electronic Resources with or without additional notice to or consent by an affected User.
- Users will be responsible for any and all damage caused by their use of Electronic Resources where such use does not comply with the requirements or purposes of this Policy. Responsibility may take the form of financial compensation, discipline, and/or restrictions on further use, as appropriate under the circumstances.

4. Duties

a. All Users

All Users have a duty to protect the security, integrity, and confidentiality of Electronic Resources, including the obligation to protect and report any unauthorized access or use, abuse, misuse, degradation, theft, or destruction. Users shall comply with this Policy and all other applicable policies, rules, and laws, when using Electronic Resources.

b. District

- District officials are responsible for designating Users authorized to use Electronic Resources.
- To the extent practical, steps shall be taken to promote the safety and security of users of the NCCVT district online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.
- The District provides for the education of students regarding the Acceptable Use Policy and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and regarding cyber-bullying awareness and response.

c. Students

Students have a duty to take reasonable steps to protect their privacy and personal information when using Electronic Resources. Students must not disclose personal contact information, except to educational institutions for educational purposes, without prior advance approval. Students also must promptly disclose to a teacher or other appropriate District employee any violation of this Policy, including any message received that the student believes to be inappropriate or makes the student feel uncomfortable.

d. Personnel

District employees are expected to communicate with students through the District-provided e-mail and are strongly advised against using other forms of personal electronic communication with students, such as Instant Messaging or texting. In the event that there is a legitimate reason for an employee to communicate with students via electronic means other than District e-mail, the employee should obtain written permission to do so from the student's parent or guardian in advance. District employees are required to take reasonable measures to protect their personal information and reputation when using Electronic Resources or otherwise participating in activity online.

5. Ownership

All Electronic Data, such as documents, data, and information that is stored, transmitted, and processed on the NCCVT Network or Electronic Resources, are the property of the District. When a User is no longer affiliated with the District as an employee, contractor, or student, all information stored by that User on any Electronic Resource remains the property of the District.

6. Unacceptable Uses

Users are prohibited from using any Electronic Resource to upload, post, mail, display, store, access, or transmit any inappropriate material or for any inappropriate purpose as set forth below. Cyber-bullying and other inappropriate online behavior off of the District network becomes the responsibility of the schools when the speech has caused or threatens to cause a substantial and material threat of disruption on campus or interference with the rights of students to be secure.

a. Access to Inappropriate Material

It shall be a violation of this Policy for any User to use any Electronic Resource to upload, post, mail, display, store, access, or transmit, any Inappropriate Material. Inappropriate Material is defined as any content, communication, or information that conflicts with the fundamental policies and mission of the District. Whether material or content is considered Inappropriate

shall be determined without regard to whether such material or content has been blocked by any filtering software used by the District. Examples of Inappropriate Material include, but are not limited to, material that:

- is hateful, harassing, threatening, libelous, or defamatory;
- is deemed offensive or discriminatory based on race, religion, gender, age, national origin, citizenship, sexual orientation, mental or physical disability, marital status, or other characteristic protected by state, federal, or local law;
- constitutes use for, or in support of, any obscene or pornographic purpose including the transmission, review, retrieval, or access to any profane, obscene, or sexually explicit material;
- constitutes use for the solicitation or distribution of information intended or likely to incite violence or to harass, threaten, or stalk another individual;
- solicits or distributes information with the intent to cause personal harm or bodily injury;
- promotes or participates in a relationship with a student that is not related to academics or school-sponsored extracurricular activities, unless authorized in advanced by the student's parent or guardian and the appropriate NCCVT official(s);
- promotes or participates in any way in religious or political activities;

b. Unlawful Purposes

It shall be a violation of this Policy for any User to use any Electronic Resource for any purpose that:

- constitutes or furthers any unlawful activity;
- gives rise to civil liability under any applicable law, including U.S. patent, trademark, or copyright laws, including copyrighted photos, clip art, or other images, including District or NCCVT logos;
- impersonates any person, living or dead, organization, business, or other entity;
- enables or constitutes gaming, wagering, or gambling of any kind;
- promotes or participates in any way in unauthorized raffles or fundraisers;
- engages in private business, commercial, or other activities for personal financial gain.

c. Security Violations

It shall be a violation of this Policy for any User to use any Electronic Resource in any way that threatens or violates the security of any Covered Technology, where such use:

- contains a virus, Trojan horse, logic bomb, malicious code, or other harmful component;
- constitutes a chain letter, junk mail, spam, or other similar electronic mail;
- constitutes unauthorized access or attempts to circumvent any security measures;
- obtains access to or use of another User's account, password, files, or data, or attempts to so access or use, without the express authorization of that other User;
- deprives a User of access to authorized access of Electronic Resources;
- engages in unauthorized or unlawful entry into a NCCVT Network;
- shares e-mail addresses or distribution lists for uses that violate this Policy or any other District Policy;
- transmits sensitive or confidential information without appropriate security safeguards;
- falsifies, tampers with, or makes unauthorized changes or deletions to data located on the NCCVT Network;
- obtains resources or NCCVT Network access beyond those authorized;
- distributes unauthorized information regarding another User's password or security data;
- discloses confidential or proprietary information, including student record information, without authorization;
- involves the relocation of hardware (except for portable devices), installation of peripherals, or modification of settings to equipment without the express prior authorization by the District Technology Department.
- installs, downloads, or uses unauthorized or unlicensed software or third-party system without the express prior authorization by the District Technology Department;
- involves a deliberate attempt to disrupt the NCCVT Network.

7. Notice of Intent to Monitor

Users have no expectation of privacy in their use of and access to any Electronic Resource. District administrators and authorized personnel monitor the use of Electronic Resources to help ensure that uses are secure and in conformity with this Policy. The District reserves the right to examine, use, and disclose any data found on the NCCVT Network in order to further the health, safety, discipline, or security of any student or other person, or to protect District property. It also may use this information in disciplinary actions and will furnish evidence of suspected criminal activity to law enforcement.

In recognition of the need to establish a safe and appropriate computing environment, the District will use filtering technology to prohibit access, to the degree possible, to objectionable or unsuitable content that might otherwise be accessible via the Internet.

8. Limitation of Liability

The District makes no warranties of any kind, neither express nor implied, for the Internet access it provides. The District will not be responsible for any damages any User suffers, including but not limited to, loss of data. The District will not be responsible for the accuracy, nature, or quality of information stored on the NCCVT Network, nor for the accuracy, nature, or equality of information gathered through District-provided Internet access. The District will not be responsible for financial obligations arising through the unauthorized use of the network.

9. Policy Violations

The District will cooperate fully with local, state, and federal officials, in any investigation related to any alleged or suspected illegal activity conducted through the NCCVT Network.

a. Due Process

Any action taken in violation of this Policy will be subject to appropriate discipline, tailored to meet the facts and circumstances of the incident. Violations of this Policy may result in the revocation or suspension of access to the NCCVT Network, as well as other disciplinary or legal action. Where a violation of this Policy also involves a violation of another District policy or rules, those policies or rules may affect the disciplinary action taken.

b. Student Violations

Violation of this Policy by a student may result in the revocation or suspension of access to the NCCVT Network, as well as other disciplinary or legal action. For a first violation, the student's parent or guardian must be contacted and a reprimand must be issued. For any subsequent violation, the student's parent or guardian must be contacted, a reprimand must be issued, and the student will be subject to disciplinary probation. Other possible actions may include any combination of the following alternatives as determined by the District: restitution, detention, probation, in-school alternative, suspension, referral to law enforcement, and expulsion. In the case of a subsequent violation, District officials also may elect to refer the student to an alternative program.

The particular consequences shall be determined by the school administrators. The Superintendent or his designee, in conjunction with the Board, shall determine when expulsion or legal action is warranted.

c. Employee Violations

Any employee who learns of or reasonably suspects a violation of this Policy is obligated to promptly report such information to his or her supervisor. Failure to do so is considered a separate violation of this Policy and, as such, may warrant disciplinary action.

Violation of this Policy by a District employee may result in the revocation or suspension of access to the NCCVT Network, as well as other disciplinary or legal action, including but not limited to: reprimand, restitution, mandatory training or in-service, and termination.

10. Social Media Guidelines

Educators have a professional image to uphold and how they conduct themselves online helps determine this image. As reported by the media, there have been instances of educators demonstrating professional misconduct while engaging in inappropriate dialogue online (i.e. blogs, wikis, social networks, texting, instant messaging) about their schools, colleagues, and/or students or posting pictures and videos of themselves engaged in inappropriate activity.

The following guidelines are intended to serve as a reference for all District personnel who elect to engage in social media, regardless of whether such online activity occurs during working or non-working time. If any employee is uncertain about how to apply these guidelines or have any question about participation in social media, he or she should seek the guidance of a supervisor or other appropriate District administrator. Administrators and certificated and/or professionally licensed employees and coaches are encouraged to use District and school-based websites or the Department of Education Home Access Center for classroom, school, school-related, or District-related instructional or informational communications with students and parents of the District. When participating in social media, personnel are bound by the following guidelines:

- The Superintendent, or his/her designee, shall create regulations for school related and/or educational/informational networking sites.

- Certificated and/or professionally licensed non-administrative employees or athletic coaches may use educational/informational networking/media sites for instructional, training, or informational purposes with the written permission of the building principal.
- The building principal must approve the continued use of the site on an annual basis and provide the Superintendent or his/her designee written verification of the sites approved by September 30 of each school year.
- No district employee may communicate with students on a social network, through email, text messages, or other web-based information and messaging sites not housed on the District Server or monitored by DTI (Delaware Department of Technology & Information) without the written permission of a student's parent(s)/legal guardian(s)/ Relative Caregiver.
- Written permission shall be given on a form created by the NCCVT School District and available to employees on the District internal website. The employee shall keep a copy of the Permission Form for his/her records.
- Employees shall not publish or distribute on any personal account maintained by the employee any personally identifiable information about students or District personnel, including but not limited to names, addresses, or photographs.
- An intentional violation of this policy or the regulations implementing this policy may lead to discipline for the employee up to and including termination of employment.