ACCEPTABLE USE POLICY FOR ELECTRONIC RESOURCES

All Danville Community School Corporation (DCSC) students and staff are responsible for their actions and activities involving the school district's computers, electronic devices, network and Internet services, and for their computer files, passwords, and accounts. These rules provide general guidance concerning the use of school computers and other electronic devices and provide examples of prohibited uses. The rules and guidelines detail acceptable use of electronic information resources under which students, staff, and all members of the DCSC community, herein referred to as "users," will be held accountable. The rules do not attempt to describe every possible prohibited activity. Students, parents, and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator. These rules apply to all school computers, all school-provided electronic devices wherever used, all uses of school servers, and Internet access and networks regardless of how they are accessed.

Acceptable Use

1. School computers, network and Internet services, and electronic resources are provided for educational purposes and research consistent with DCSC's educational mission, curriculum, and instructional goals.
2. Users must comply with all school board policies, the student handbook, and school rules and expectations concerning conduct and communication when using school computers or school-issued electronic resources, whether on or off school property.
3. Students also must comply with all specific instructions from school staff.

Prohibited Uses

Unacceptable uses of school electronic resources include, but are not limited to, the following:

1. Accessing or Communicating Inappropriate Materials – Users may not access, submit, post, publish, forward, download, scan, or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying, and/or illegal materials or messages.
2. Illegal Activities – Users may not use the school district's computers, electronic devices, networks, or Internet services for any illegal activity or in violation of any board policy/procedure or school rules. DCSC and its employees and agents assume no responsibility for illegal activities of students while using school computers or school-issued electronic resources.
3. Violating Copyrights or Software Licenses – Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is prohibited, except when the use falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.
4. Plagiarism – Users may not represent as their own work any materials obtained on the Internet (ie: term papers, articles, music, etc). When using other sources, credit must be given to the copyright holder.

5. Use for Non-School-Related Purposes - School district's computers, electronic devices, and network and Internet services are provided for purposes related to educational programs, school operations, and performance of job responsibilities. Incidental personal use of school devices is permitted as long as such use: 1) does not interfere with the user's responsibilities and performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules or any other board policy, procedure, or school rules. "Incidental personal use" is defined as use by an individual for occasional personal communications.
6. Misuse of Passwords/Unauthorized Access – Users may not share passwords, use other users' passwords, access or use other users' accounts, or attempt to circumvent network security systems.
7. Malicious Use/Vandalism – Users may not engage in any malicious use,disruption, or harm to the school district's computers, electronic devices, or network and Internet services, including but not limited to hacking activities and the creation/uploading of computer viruses.
8. Avoiding School Filters – Users may not attempt to or use any software, utilities, or other means to access Internet sites or content blocked by the school filters.
9. Unauthorized Access to Blogs/Social Networking Sites, Etc. – Users may not access blogs, social networking sites, etc. prohibited by building administration or the DCSC Technology Department. Teachers and students using authorized social networking sites for educational projects or activities shall follow the age requirements and legal requirements that govern the use of social networking sites in addition to the guidelines established in this policy.
10. Wasting System Resources - Users shall not use the network in such a way that would waste system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming not directly related to educational projects as determined by the supervising instructor or building administrator.
11. Unauthorized Equipment - Users may not attach unauthorized equipment, including personal laptops, tablets, and handheld devices, to the district network without permission from the DCSC Technology Department.

Compensation for Losses, Costs, and/or Damages

As technology has become more mobile many electronic devices owned by the Danville Community School Corporation and used by staff members are transported outside both the direct physical control and locations controlled by the Danville School Corporation. It is in this outside environment that responsibility is shared by both the Danville School Corporation and the individual staff member who chooses to take an electronic device off school grounds. In the event that an electronic device is lost, stolen, or damaged the individual staff member is responsible for up to $100 per electronic device. In addition all users (students and staff) may be responsible for compensating the school district for any losses, costs, or damages incurred for

violations of board policies/procedures and school rules. The school district assumes no responsibility for any unauthorized charges or costs incurred by users while using school district computers, devices, or the school network.

Staff Uses of Social Media or Social Networking Website

Danville Community School Corporation respects the right of employees to use social media networking sites, personal websites, blogs, tweets, and other forms of electronic communication. It is important that school employees' personal or professional use of these sites does not damage the reputation of the school, its staff, students, or their families. Employees should exercise care in setting appropriate boundaries between their personal and public online behavior, understanding what is private in the digital world. Such online behavior always has the possibility of becoming public, even without knowledge or consent.
Danville Community School Corporation asks all employees to carefully review the privacy settings on any social media and networking sites they use (ie: Facebook, MySpace, Twitter, Flickr, LinkedIn, etc.) and exercise care and good judgment when posting school content and information. In addition school employees should adhere to the following policies, which are consistent with the school's workplace standards on harassment, student relationships, conduct, professional communication, and confidentiality:

1. An employee should not make statements that would violate any of the school's policies, including its policies concerning discrimination, harassment, content, and confidentially.
2. All school employees must uphold Danville Community School Corporation's value of respect for the individual and avoid making defamatory statements concerning the school, its employees, its students, or their families.
3. An employee may not disclose any confidential school information or confidential information obtained during the course of his/her employment concerning any individuals or organizations, including staff, students, and/or their families.
4. All sites established or maintained by Danville Community School employees that can be identified, or could reasonably be construed as a Danville Community School Corporation site, are deemed the property of the Danville Community School Corporation.
5. At no time may a student(s) name(s) or other identifying information be matched with a student's picture or likeness without express written permission of the parent or guardian.
6. When establishing a social networking site that represents Danville Community School Corporation, all school employees must follow the Danville Community School Corporation prescribed naming convention.

7. School employees who create sites to be used by students may not include any resources that students are forbidden to access at school.
8. All websites/social networking sites created or maintained by school employees are the direct responsibility of that employee and should be kept up-to-date and continually monitored and appropriately edited in a timely fashion by the sponsoring employee.
9. Danville Community School Corporation will provide employees a set of guidelines designed to aid in the creation, appropriate use, monitoring, and interactions on social websites and when dealing with electronic communications.
10. Any Danville Community School employee upon departure from Danville Community school Corporation must release to Danville Community School Corporation access and control of any website/social networking site established as a Danville Community School Corporation site.

For more detailed information and employee guidelines for developing, maintaining, and other social networking practices, please see Danville Social Networking guidelines.

Student Security
Users may not reveal personal information, including a home address and phone number, about themselves or another individual on any unsecured electronic medium, such as web sites, blogs, podcasts, videos, wikis, or social networking sites. If users encounter dangerous or inappropriate information or messages, they shall notify the school administration immediately.

Staff may post student pictures on district/ school/classroom “public” websites as long as the student’s name or other identifying information is not included. Students’ grades, test results, or identifying pictures may be stored only on district-approved secure sites that require a username and password for authorized individuals to access.

All Danville Community Schools are closed campuses. DCSC retains all rights concerning any recording and/or publishing of any student’s or staff member’s work(s) or image(s). Students must obtain permission from a DCSC staff member to publish a photograph or video of any school-related activity. It is best practice and common courtesy to ask permission before recording an individual or groups.

The use of cameras on any type of electronic device is strictly prohibited in locker rooms and restrooms.

DCSC staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

Students may be issued a school email address to improve student communication and

collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment.

Technology Privacy
All computers, telephone systems, voicemail systems, electronic mail, and electronic communication systems are the district's property. The district retains the right to access and review all electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with district's computer system, telephone system, electronic mail system, and voice mail system. Students and staff should have no expectation that any information contained on such systems is confidential or private.

System Security
Any user who identifies a security problem must notify his/her teacher or building administrator immediately. The user shall not demonstrate the problem to others or access unauthorized material. Staff shall immediately report any potential security breaches to the DCSC Technology Department.

Staff shall change their passwords to all systems at least once every 90 days.

Personal Devices
All users are prohibited from using privately-owned electronic devices in school unless explicitly authorized by the building principal or DCSC district administration.

Additional Rules for Laptops, iPads, or other Electronic Devices Issued to Students or Staff

1. Electronic devices loaned or leased to students or staff shall be used only for educational purposes that directly relate to a school project or assignment, unless otherwise explicitly authorized by building administration.
2. Users are responsible for the proper care of electronic devices at all times, whether on or off school property, including costs associated with repairing or replacing the device.
3. Users must report a lost or stolen device to the building administration immediately. If a device is stolen, a report also should be made immediately with the school safety officer and/or local police.
4. The policy and rules apply to the use of the electronic device at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of devices issued by school staff.
5. Violation of policies or rules governing the use of electronic devices or any careless use of the device may result in a student's device being confiscated and/or a student only being allowed to use the device under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies/procedures or school rules.
6. Parents are responsible for supervising their child's use of the device when not in

school.

7. The device configuration shall not be altered in any way by users; this includes software, hardware and accessories such as cases. No software applications shall be installed, removed, or altered on the device unless permission is explicitly given by the teacher or building administrator.
8. The device is to be used only by the student or staff member to whom it is issued. The person to whom the device is issued will be responsible for any activity or action performed on the device.
9. The device must be returned in acceptable working order by the last day of each school year, upon withdrawal or exit date from the school district, and whenever requested by school staff.

Terms of Use

DCSC reserves the right to deny, revoke, or suspend specific user privileges and/or take other disciplinary action, including suspensions or expulsion from school, for violations of this policy. Additionally, all handbook regulations apply to the use of the DCSC network, Internet, and electronic resources.

Disclaimer – DCSC, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, Internet access, and electronic resources it is providing. Furthermore, DCSC is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.
2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.
3. Unauthorized financial obligations resulting from the use of DCSC electronic resources.