Northeastern Clinton Central School District

Internet and Technology Acceptable Use Policy

Revised:

- August 30, 2017
- Revised Media Release Form - July 6, 2018
- Opt Out AUP Form – August 2019
- September 10, 2019

103 Route 276
Champlain, New York
Telephone: 518-298-8242 Fax: 518-298-4293

Northeastern Clinton Central School District

Internet and Technology Acceptable Use Policy

The Northeastern Clinton Central School District ("District") maintains the District's Computer System ("DCS") for educational purposes, classroom and communication activities, and career and professional development for use by its students, faculty, and staff members. The DCS consists of software, hardware, computer networks and electronic communication systems, including, but not limited to, cloud-based computing platforms. The DCS provides internet, e-mail, and access to printing and data storage in a secure environment.

The DCS may only be used for school-related work or activities and may not be used for any illegal purpose. Access to the DCS is a privilege granted only by the District. User access to the DCS or any of its components may be withdrawn by the District at any time, with or without notice to the user.

I. General Terms and Conditions of Use

A. Purpose of Technology

The District provides the DCS to users as a privilege and solely for educational purposes. The District provides the DCS to allow for global access for students and staff beyond the confines of the classroom, providing many opportunities to promote educational merit through facilitating resource sharing, innovation, and communication supported by parents, guardians, and District staff.

The District has adopted this **Internet and Technologies Acceptable Use Policy ("Policy") to set forth rules and expectations with regard to use of the DCS**. In addition, the District recognizes the following in providing District Internet and technological access: Family Educational Rights and Privacy Act (FERPA), Children's Internet Protection Act (CIPA), Individuals with Disabilities Education Act (IDEA), and Children's Online Privacy Protection Act (COPPA).

B. Technology Opportunity & Risks and Security

The use of technology may expose users to material that does not have any educational value, or that may be harmful or disruptive. The District cannot predict or control material that user's access. However, the District believes the educational value of accessing information, interacting with others, and conducting research through District technology outweighs the possibility that users may obtain or gain access to material not consistent with District educational goals.

In accordance with the Children's Internet Protection Act (CIPA), the District has installed and manages filtering software to limit users' Internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, or disruptive to the District's educational process or goals, notwithstanding that such software may, in some instances, block access to other material as well. The District cannot guarantee that filtering software will in all instances successfully block access to materials not consistent with District goals.

The use of filtering software does not negate or otherwise affect the responsibilities of the users to follow as outlined within this Policy. It is important that users realize this and recognize their responsibility to act appropriately while using the District computer network. District users must conduct themselves accordingly by exercising good judgement and complying with District policy. District network users are responsible for their behavior and communications using the District's technology and networks.

Any statement accessible on the DCS is understood to be the author's individual point of view and not necessarily that of the District. A student's parents or guardians are responsible for monitoring the student's use of District technology from home.

In addition to filtering, the District recognizes the importance of supervision of students due to filtering limitations. Staff are responsible for monitoring and supervising student users of the DCS (including Internet access).

Lastly, District staff will provide education to students about technology such as online behavior, interacting with email, forums, chat rooms, social networking sites, cyberbullying and other Internet related issues each school year. District staff will also receive training on these issues during District professional development.

C. No Expectation of Privacy

The DCS is the District's property and its use is subject to the District's policies. **Users do not have any expectation of privacy when using the DCS, including messages sent, received, or stored on District email systems or in use of the Internet, and including when using personal devices or BYOD (Bring Your Own Device) to use the DCS.** The District has the right to monitor all aspects of the DCS, including but not limited to, data saved on the DCS; monitoring of sites accessed through the DCS; and reviewing e-mails sent or received by users of the DCS.

D. Prohibited Activities

All students and staff must abide by the District's Code of Conduct and Policies when using the DCS. No one shall use DCS to access or attempt to access material that is profane or obscene (such as pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (such as hate literature). DCS users who inadvertently access such material must immediately consult an administrator (or, in the case of student users, a teacher or administrator) and notify them of the inadvertent access.

The following are not permitted:

- DCS users will not attempt to gain access to any element of the DCS that is beyond their authorized access.
- DCS users will not make deliberate attempts to disrupt the DCS, override security, destroy data, or spread computer viruses, malware, or spyware. DCS users may not act in such a way so as to disrupt the use of the DCS by others. The DCS shall not be destroyed, modified, or abused in any way.
- Malicious use of the DCS to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
- Unauthorized installation of any software, including shareware and freeware, for use on the DCS is prohibited.
- Downloading, copying, or duplicating, and/or distributing copyrighted materials without specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).
- Establishing network or Internet connections to live communications, including voice and/or video (relay chat), is prohibited unless specifically authorized by the building principal, NERIC staff, or a classroom teacher.
- DSC users are not permitted to store, send, or display offensive messages or pictures, use obscene or vulgar language, or harass, insult, or attack other individuals.
- DCS users are responsible for their individual accounts and must take all reasonable precautions to prevent others from being able to use their accounts. Providing another individual with your username and password is a serious violation.
- DCS users must follow District virus protection procedures prior to opening files or file attachments from a non-district storage device, i.e. flash/USB or external drives.

- It is required that all DCS users change their passwords every three (3) months to ensure the security of the District's network.
- If DCS users leave their computer/device for any reason, they must lock or log off their system to ensure user profile and network integrity.
- District staff must notify the Northeastern Regional Information Center ("NERIC") personally if they identify any type of security concern.
- Students must notify classroom teacher or building administrator if they identify with any type of security concerns.

II. Staff Responsibilities

A. Staff Email

District staff are provided with District email accounts to improve effectiveness and efficiency of communication both within the District and parties outside the district and broader community.

District staff must abide by the following expectations when using District email:

- Staff must use District email when communicating with students, parents, and other individuals for matters related to District business. The use of personal email accounts for communication with students or parents or other individuals for matters related to District business is prohibited.
- Staff emails to parents/guardians must be professional in nature and use appropriate grammar, format, and salutations.
- Staff emails to students may only be sent to students' District email accounts and must abide by professional standards for conduct and may only be used to conduct District business.
- Staff will not access, forward or respond to email "chainmail", spam, or phishing attempts; and will not click on any links or attachments in such emails. The District will never request or require personal or District account information via e-mail.

B. Staff Personal Device Use (BYOD)

- The District reserves the right to determine which personal devices, if any, may be used to access the DCS, with authorization from building principals and NERIC Staff.
- Users may not utilize any personal device in a manner that is disruptive to any other user.
  The District is not responsible for any damage to personal devices. Users may be held responsible for any District hardware or network replacement or repair costs caused by their personal device.

C. Staff Acceptance Agreement

Computers and/or other technology devices provided to staff for school-related and professional use are property of the District. District employees will complete and follow the "District Employee Computer Acceptance Agreement" upon receiving a District device. Employees must complete the online agreement form found on the District's website within 24 hours of device receipt. This form may be found at http://bit.ly/2A2wYuP.

D. Violations for Improper Use and/or Access

Staff who improperly access the DCS or misuse District technology may be subject to discipline, up to and including termination, in accordance with their respective collective bargaining agreements and/or the District's discretion.

103 Route 276
Champlain, New York
Telephone: 518-298-8242 Fax: 518-298-4293

III. Student Responsibilities

A. Student Opt-In Program for Access to District Technology

The District recognizes the importance of the Internet and network resources as an integral part of learning and advancing the mission of the District. The District provides technology for educational purposes, classroom and communication activities, career and professional development to increase communication of knowledge on global issues and awareness and research to build 21st life-long learners.

Students shall be annually AUTOMATICALLY opted-in to the District's network, internet, and technology. This means that students will have IMMEDIATE access to all District internet and technology starting the first day of school. If you DO NOT want your student to have Internet or network access, please complete the **District's Internet and Technologies Use Policy Opt-Out Form** and return to your homeroom teacher no later than September 30, 2019, and access will be revoked.

Please be advised that when classroom tasks require Internet access for the instructional process, alternatives will be provided to the student, but this will exceedingly limit the student's ability to participate and complete classroom tasks, and may be a detriment to the student's education.

Additionally, the District requires that all students accessing the internet and/or utilizing District technology to sign and return the following forms (attached to this policy) to your assigned homeroom teacher no later than September 30, 2019:

- The District's Media Release Form;
- The Student Network Agreement Form;
- The Parent/Guardian Network Agreement Form; and,
- The Student Opt-Out Form (If choosing to opt-out of the DCS).

Students and their parents/guardians should familiarize themselves with this Policy **each year**.

B. Student Email

Students in Grades 6 – 12 are provided District email accounts for educational purposes and to promote effective communication between among the District community. Access to District email accounts is a privilege and students must follow District guidelines and the District Code of Conduct when utilizing email accounts.

Students may only use District email for school-related purposes, such as communicating and collaborating with teachers and students regarding school work. Students may not use District email for any other purpose, and may not use District email in any way which constitutes a violation of the District Code of Conduct. Students must report any use of District email which violates the District Code of Conduct to a teacher or administrator immediately.

C. Student Personal Device Use

The District recognizes technology is continually emerging (tablets, eBooks, cell phones, etc.) and the potential for technology to enhance the classroom learning environment. Students may use these personal devices during the school day when granted permission by an administrator or teacher under the following conditions:

- Personal device use is a privilege that may be revoked at any time. Any personal device that may create a distraction, audible or otherwise, must be off unless permission is granted by an administrator or teacher.

- Students may not use a personal device at times or in ways that, in a teacher's judgement, may interfere with learning process.
- Personal devices may be confiscated if they are used inappropriately.
- If use of a personal device is not permitted, it should be stored where the teacher deems appropriate.
- The District is not responsible for any personal device data plan charges, lost or damaged devices, or stolen property.

District administration has the authority to further restrict possession of personal devices to be consistent with building level policies.

D. Student Device Care

Computers and/or other technology devices provided to students for school-related and professional use are property of the District.

Upon delivery or issuance of a computer/device to a student, the student and/or his or her parents or guardians are responsible for the computer/device at all times that the computer/device is signed out to the student. Students and their parents or guardians must take reasonable care to protect and properly use the computer/device. Students will follow the following precautions when using District computers/devices:

- Students are responsible for the general care of their computer/device that they are assigned and/or using within the District.
- If a computer/device is broken or fails to operate properly, the student must immediately contact the teacher or NERIC staff for evaluation of the technology device.
- Please carefully insert only designated cords and cables into the computer/device to prevent damage.
- Students are responsible for bringing their computers/devices fully charged with all assigned apparatuses daily.
- Transporting of computers/devices must be within the District provided carrying cases; please do not place anything on the top of the computer/device to prevent screen damage, screens are sensitive to damage with excessive pressure on the screen.
- When cleaning a computer/device, use a soft, dry cloth or anti-static, without any cleaner of any type if not approved by the District.
- Computers/devices should not be operated while consuming food or drink.
- Computers/devices must be stored in a locked locker and never left unattended or unsupervised.
- Computers/devices may not be left in environments with extreme cold or heat as such actions may damage or make technology inoperable.
- Computers/devices must be free from all writings or markings other than that provided by the District; District labels or asset tags may not be removed from computers/devices.
- Computers/devices are the responsibility of the student issued the technology, who is therefore the only authorized user. Computers/devices may not be shared or traded with other individuals including other students, parents, guardians, or school staff.
- Students are only permitted to adhere items to the device that can be easily removed without damaging the device or leaving a residue."

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)
NOTICE REGARDING ACCESS TO STUDENT RECORDS AND STUDENT INFORMATION

Dear Parent or Eligible Student:

This is to advise you of your rights with respect to student records pursuant to the Family Educational Rights and Privacy Act (FERPA). FERPA is a federal law designed to protect the privacy of student records. The law gives parents and students over 18 years of age (referred to in the law as "eligible students") the following rights:

1. **The right to inspect and review the student's education records within 45 days of the day the district receives a request for access.** Parents or eligible students should submit to the Building Principal a written request that identifies the records they wish to inspect. The Principal will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.
2. **The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate or misleading.** Parents or eligible students may ask the district to amend a record that they believe is inaccurate or misleading by writing the Principal, clearly identifying the part of the record they want changed, and specifying why it is inaccurate or misleading.

If the district decides not to amend the record as requested by the parent or eligible student, the district will notify the parent or eligible student of the decision and advise them of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

3. **The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent.** The exceptions, which permit disclosure without consent, are disclosure to school officials with legitimate educational interests or an authorized representative. A school official is a person employed by the district as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel); a person serving on the school board; a person or company with whom the district has contracted to perform a special task (such as an attorney, auditor, medical consultant, or therapist); or a parent or student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

An authorized representative is any individual or entity designated by a State or local educational authority or a Federal agency headed by the Secretary, the Comptroller General or the Attorney General to carry out audits, evaluations, or enforcement or compliance activities relating to educational programs.

Upon request, the district discloses education records without consent to officials of another school district in which a student seeks or intends to enroll.

4. **The right to file a complaint with the U.S. Department of Education concerning alleged failures by the district to comply with the requirements of FERPA.** The Office that administers FERPA is:

Family Policy Compliance Office
U.S. Department of Education
600 Independence Avenue SW
Washington, DC 20202-4605

NOTIFICATION OF DIRECTORY INFORMATION DESIGNATIONS

In addition to the rights outlined above, FERPA also gives the school district the option of designating certain categories of student information as "directory information." Directory information includes student*[include only those designated as directory information]*:

- Name
- ID number, user ID, or other unique personal identifier used by a student for purposes of accessing or communicating in electronic systems (only if the id cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the student's identity),
- Address
- Telephone number
- Date and place of birth
- Major course of study
- Participation in school activities or sports
- Weight and height if a member of an athletic team
- Dates of attendance
- Degrees and awards received
- Most recent school attended
- Grade level
- Photograph,
- E-mail address
- Enrollment status

You may object to the release of any or all of this "directory information." However, you must do so in writing within 10 business days of receiving this notice. If we do not receive a written objection, we will be authorized to release this information without your consent. For your convenience, you may note your objections to the release of directory information on the enclosed form and return it to the Building Principal.

Sincerely,

{Insert Building Principal's Name Here}