

## **APPROVED 2017 UPDATED GUIDELINE**

### **STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Students shall use School Corporation Technology Resources (see definition in Bylaw 0100) for educational purposes only. Corporation Technology Resources shall not be used for personal, non-school related purposes. Use of Corporation Technology Resources is a privilege, not a right. When using Corporation Technology Resources, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Students found to have engaged in unauthorized or inappropriate use of Corporation Technology Resources, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action consistent with the Student Handbook, and/or civil or criminal liability. Prior to accessing or using Corporation Technology Resources, students and parents of minor students must sign the Student Technology Acceptable Use and Safety Agreement (Form 7540.03 F1). Parents should discuss their values with their children and encourage students to make decisions regarding their use of Corporation Technology Resources that is in accord with their personal and family values, in addition to the School Board's standards.

This guideline also governs students' use of their personal communication devices (see definition in Bylaw 0100) when they are connected to Corporation Technology Resources or while the student is on Corporation-owned property or at a Corporation-sponsored activity.

Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using Corporation Technology Resources.

- A. All use of Corporation Technology Resources must be consistent with the educational mission and goals of the Corporation.
- B. Students may access Corporation Technology Resources only by using their assigned account and may send only school-related electronic communications using their Corporation-assigned e-mail addresses. Use of another person's account/e-mail address is prohibited. Students shall not allow other users to utilize their passwords. Students may not go beyond their authorized access. Students should take steps to prevent unauthorized access to their accounts by logging off or "locking" their computers, laptops, tablets, and personal communication devices when leaving them unattended.
- C. No user may have access to another's private files. Any attempt by users to access another user's or the Corporation's non-public files, or voicemail or e-mail messages is considered theft. Attempts to gain access to unauthorized resources or information either on the Corporation's computer or telephone systems or any systems to which the Corporation has access are prohibited. Similarly, students shall not intentionally seek information on, obtain copies

of, or modify files, data or passwords belonging to other users, or misrepresent other users on the network.

- D. Students shall not intentionally disable any security features used on Corporation Technology Resources.
- E. Students shall not use Corporation Technology Resources or their personal communication devices to engage in vandalism, "hacking," or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; sale of illegal substances and goods).
  - 1. Slander and libel – - In short, slander is “oral communication of false statements injurious to a person’s reputation,” and libel is “a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person’s reputation or the act or an instance of presenting such a statement to the public.” (The American Heritage Dictionary of the English Language. Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Students shall not knowingly or recklessly post false or defamatory information about a person or organization. Students are reminded that material distributed over the Internet is “public” to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.
  - 2. Students shall not use Corporation Technology Resources to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation or transgender identity, age, disability, religion, or political beliefs. Sending, sharing, viewing or possessing pictures, text messages, e-mails or other materials of a sexual nature (i.e. sexting) in electronic or any other form, including the contents of a personal communication device or other electronic equipment is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.
  - 3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or information residing in Corporation Technology Resources or any computer system attached through the Internet is strictly prohibited. In particular, malicious use of Corporation Technology Resources to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage

the software components of a computer or computing system is prohibited.

Attempts to violate the integrity of private accounts, files or programs, the deliberate infecting of the network or computers, laptops, tablets, etc., attached to the network with a "virus", and attempts at hacking into any internal or external computer systems using any method will not be tolerated.

Students shall not engage in vandalism or use Corporation Technology Resources or their personal communication devices in such a way that would disrupt others' use of Corporation Technology Resources.

Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creating computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Students also must avoid intentionally wasting limited resources. Students must notify the teacher, building principal, or appropriate staff member immediately if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

4. Students shall not use Corporation Technology Resources to access, process, distribute, display or print prohibited material at any time, for any purpose. Students may access, process, distribute, display or print restricted material, and/or limited access material only as authorized below.
  - a. Prohibited material includes material that constitutes child pornography and material that is obscene, objectionable, inappropriate and/or harmful to minors, as defined by the Children's Internet Protection Act. As such, the following material is prohibited: material that appeals to a prurient or unhealthy interest in nudity, sex, and excretion; material that depicts, describes, or represents in a patently offensive way (with respect to what is suitable for minors) an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political or scientific value as to minors. Prohibited material also includes material

that appeals to a prurient or unhealthy interest in or depicts, describes, or represents in a patently offensive way violence, death, or bodily functions; material designated as for “adults only”; and material that promotes or advocates illegal activities.

- b. Restricted material shall not be accessed by elementary or middle school students at any time, for any purpose. Restricted material may be accessed by high school students in the context of specific learning activities that have been approved by a teacher or staff member for legitimate research purposes. Materials that arguably may fall within the description provided for prohibited material that have clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be restricted. In addition, restricted material includes materials that promote or advocate the use of alcohol and tobacco, hate and discrimination, satanic and cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are restricted unless such sites have been specifically approved by the teacher and principal.
- c. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities that are directed by a teacher or during periods that a school may designate as “open access” time. Limited access material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investment.

If a student inadvertently accesses material that is considered prohibited or restricted, s/he must disclose the inadvertent access to the teacher or building principal immediately. This will protect the student against an allegation that s/he intentionally violated the provision.

The determination of whether material is prohibited, restricted, or limited access shall be based on the content of the material and the intended use of the material, not on the protective actions of the technology protection measures. The fact that the technology protection measures have not protected against access to certain material shall not create the presumption that such material is appropriate for students to access. The fact that the technology protection measures have blocked access to certain material shall not

create the presumption that the material is inappropriate for students to access.

5. Unauthorized Use of Software or Other Intellectual Property from Any Source – All communications and information accessible via the Internet should be assumed to be private property (i.e., copyrighted and/or trademarked). Laws and ethics require proper handling of intellectual property. All copyright issues regarding software, information, and attributions/acknowledgement of authorship must be respected.

Software is intellectual property, and, with the exception of freeware, is illegal to use without legitimate license or permission from its creator or licensor. All software loaded on Corporation computers must be approved by the Technology Director, and the Corporation must own, maintain, and retain the licenses for all copyrighted software loaded on Corporation computers. Students are prohibited from using Corporation Technology Resources for the purpose of illegally copying another person's software. Illegal peer-to-peer file trafficking of copyrighted works is prohibited.

Online articles, blog posts, podcasts, videos, and wiki entries are also intellectual property. Students should treat information found electronically in the same way they treat information found in printed sources – i.e., properly citing sources of information and refraining from plagiarism. Rules against plagiarism will be enforced.

- F. Transmission of any material in violation of any State or Federal law or regulation or Board policy is prohibited.
- G. Corporation Technology Resources may not be used for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by students), advertising, or political lobbying.
- H. Use of Corporation Technology Resources to engage in cyberbullying is prohibited. "Cyberbullying" involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, which is intended to harm others. [Bill Belsey (<http://www.cyberbullying.org>)] Cyberbullying may occur through e-mail, instant messaging (IM), chat room/Bash Boards, small text-messages (SMS), websites, and voting booths.

Cyberbullying includes, but is not limited to the following:

1. posting slurs or rumors or other disparaging remarks about a student on a website or on weblog;
  2. sending e-mail or instant messages that are mean or threatening or so numerous as to negatively impact the victim's use of that method of communication and/or drive up the victim's cell phone bill;
  3. using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings of students;
  4. posting misleading or fake photographs of students on websites.
- I. Students are expected to abide by the following generally-accepted rules of network etiquette:
1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through or utilizing Corporation Technology Resources. Do not use obscene, profane, vulgar, sexually explicit, defamatory, threatening, abusive or disrespectful language in communications made through or utilizing Corporation Technology Resources.
  2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.
  3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending him/her messages, the student must stop.
  4. Do not post information that, if acted upon, could cause damage or a danger of disruption.
  5. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet. This prohibition includes, but is not limited to, disclosing personally identifiable information on commercial websites.
  6. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.
  7. Never agree to get together with someone you "meet" on-line without prior parent approval and participation.

8. Check e-mail frequently, and delete e-mail promptly.
  9. Students should disclose promptly to a teacher or administrator any messages they receive that are inappropriate or make them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). Students should not delete such messages until instructed to do so by an administrator.
- J. Downloading of files onto school-owned equipment or contracted online educational services is prohibited, without prior approval from the classroom teacher; all downloads must be to an external storage device. If a student transfers files from information services and electronic bulletin board services, the student must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or software program that infects Corporation Technology Resources with a virus and causes damage, the student will be liable for any and all repair costs to make the Corporation Technology Resources once again fully operational.
- K. Students must secure prior approval from a teacher before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or "Listservs."
- L. Students are prohibited from accessing or participating in online "chat rooms" or other forms of direct electronic communication (e.g., instant messaging) (other than e-mail) without prior approval from a teacher or the Principal. All such authorized communications must comply with these guidelines. Students may use their school-assigned accounts/email addresses only when accessing, using or participating in real-time electronic communications for education purposes.
- M. Users have no right or expectation to privacy when using the Corporation Technology Resources. The Board reserves the right to access and inspect any facet of its Technology Resources, including, but not limited to, computers, laptops, tablets, and other web-enabled devices, networks, Internet connections or online educational apps or services, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein. A student's use of Corporation Technology Resources constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the Technology Resources and related storage medium and equipment. Routine maintenance and

monitoring, utilizing both technology monitoring systems and staff monitoring, may lead to discovery that a user has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated Board policy and/or the law or if requested by local, State or Federal law enforcement officials. Students' parents have the right to request to see the contents of their children's files, e-mails and records.

- O. Use of the Internet and any information procured from the Internet is at the student's own risk. The Corporation makes no warranties of any kind, either express or implied, that the functions or the services provided by or through Corporation Technology Resources will be error-free or without defect. The Corporation is not responsible for any damage a user may suffer, including, but not limited to, loss of data, service interruptions, or exposure to inappropriate material or people. The Corporation is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects must be cited the same as references to printed materials. The Corporation is not be responsible for financial obligations arising through the unauthorized use of its Technology Resources. Students or parents of students will indemnify and hold the Corporation harmless from any losses sustained as the result of a student's misuse of Corporation Technology Resources.
- P. Disclosure, use and/or dissemination of personally identifiable information of minors via the Internet is prohibited except as expressly authorized by the minor student's parent/guardian on the "Student Technology Acceptable Use and Safety Agreement Form."

Proprietary rights in the design of web sites hosted on the Corporation's servers remains at all times with the Corporation.

- R. File-sharing is strictly prohibited. Students are prohibited from downloading and/or installing file-sharing software or programs on Corporation Technology Resources.

Students may not use Corporation Technology Resources to establish or access web-based e-mail accounts on commercial services (e.g., Gmail, iCloud, Outlook, Yahoo mail, etc.) unless the account is issued and maintained by the School Corporation

- T. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the Corporation's users will be investigated fully and disciplinary action will be taken as appropriate.

- U. Preservation of Resources and Priorities of Use: Corporation Technology Resources are limited. Each student is permitted reasonable space to store e-mail, web, and personal school-related files. The Board reserves the right to require the purging of files in order to regain disk space. Students who require access to Corporation Technology Resources for class- or instruction-related activities have priority over other users. Students not using Corporation Technology Resources for class-related activities may be “bumped” by any student requiring access for class- or instruction-related activities. The following hierarchy will prevail in governing access to Corporation Technology Resources:

1. Class work, assigned and supervised by a staff member.
2. Class work, specifically assigned but independently conducted.
3. Personal correspondence (e-mail – checking, composing, and sending).
4. Training (use of such programs as typing tutors, etc.).
5. Personal discovery (“surfing the Internet”).
6. Other uses – access to resources for “other uses” may be further limited during the school day at the discretion of the building principal or teachers.

Game playing is not permitted unless under the supervision of a teacher.

### **Abuse of Network Resources**

Peer-to-peer file sharing, mass mailings, downloading of unauthorized games, videos, and music are wasteful of limited network resources and are forbidden. In addition, the acquisition and sharing of copyrighted materials is illegal and unethical.

### **Unauthorized Printing**

Corporation printers may be used to print only school-related documents and assignments. Printers, like other school resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement are very expensive. The Corporation monitors printing by user. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the student. Users are prohibited from replacing ink cartridges and performing any other service or repairs to printers. Users should ask, as appropriate, for assistance to clear paper that is jamming a printer.

Any questions and concerns regarding these guidelines may be directed to classroom teachers or building Principals.

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended

20 U.S.C. 6301 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended

18 U.S.C. 2256

18 U.S.C. 1460

18 U.S.C. 2246

20 U.S.C. 6777, 9134 (2003)

© **NEOLA 2017**