Book	Administrative Guideline Manual
Section	7000 Property
Title	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	ag7540.03
Status	Active
Adopted	June 1, 2006
Last Revised	November 3, 2017

7540.03 - **STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Students shall use District Technology Resources (see definition Bylaw 0100) for educational purposes only. District Technology Resources shall not be used for personal, non-school related purposes. Use of District Technology Resources is a privilege, not a right. When using District 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 District 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 District 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 District Technology Resources that is in accord with their personal and family values, in addition to the Board's standards. Students must complete a mandatory training session/program as part of being assigned a school e-mail address.

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

A. All use of District Technology Resources must be consistent with the educational mission and goals of the District.

B. Students may only access and use District Technology Resources by using their assigned account and may only send school-related electronic communications using their District-assigned e-mail addresses. Use of another person's account/e-mail address is prohibited. Students may not allow other users to utilize their account/e-mail address and should not share their password with other users. 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/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 District's non-public files, or phone or e-mail messages is considered theft. Any attempts to gain access to unauthorized resources or information either on the District's computer or telephone systems or any systems to which the District has access are prohibited. Similarly, students may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the District's Network.

D. Students may not intentionally disable any security features used on District Technology Resources.

E. Students may not use District 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 District 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 District Technology Resources or any computer system attached through the Internet is strictly prohibited. In particular, malicious use of District 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", attempts at hacking into any internal or external computer systems using any method will not be tolerated.

Students may not engage in vandalism or use District Technology Resources or their personal communication devices in such a way that would disrupt others' use of District 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 creation of 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 immediately notify the teacher, Administrator, or Technology Manager 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. Use of District Technology Resources to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient 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. If a student inadvertently accesses material that is prohibited by this paragraph, s/he should immediately disclose the inadvertent access to the teacher or Building Director. This will protect the user against an allegation that s/he intentionally violated this provision.

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 District computers must be approved by the Technology Director, and the District must own, maintain, and retain the licenses for all copyrighted software loaded on District computers. Students are prohibited from using District 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.

6. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

7. District 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. This provision shall not limit the use of District Technology Resources for the purpose of communicating with elected representatives or expressing views on political issues.

8. Use of District 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, voting booths.

   Cyberbullying includes, but is not limited to the following:

   a. posting slurs or rumors or other disparaging remarks about a student on a website or on weblog;

   b. 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;

   c. using a camera phone to take and send embarrassing and/or sexually explicit photographs/recordings of students;

   d. posting misleading or fake photographs of students on websites.

9. Students are expected to abide by the following generally-accepted rules of online etiquette:

   a. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through or utilizing District Technology Resources Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive or disrespectful language in communications made through or utilizing District Technology Resources.

   b. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

   c. 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.

   d. Do not post information that, if acted upon, could cause damage or a danger of disruption.

   e. 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 personal identification information on commercial websites.

   f. Do not transmit pictures or other information that could be used to establish your identity without prior approval of a teacher.

   g. Never agree to get together with someone you "meet" on-line without parent approval and participation.

h. Check e-mail frequently, and delete e-mail promptly.

i. Students should promptly disclose 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.

H. Downloading of files onto school-owned equipment or contracted online educational services is prohibited, without prior approval from the Wayne County Schools Career Center. 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 installs a software program that infects District Technology Resources with a virus and causes damage, the student will be liable for any and all repair costs to make the District Technology Resources once again fully operational.

I. Students must secure prior approval from a teacher or the Wayne County Schools Career Center before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or Listservs.

J. Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, Superintendent, or Building Director. Students may only use their school-assigned accounts/email addresses 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 District 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, or Internet connections or online educational services or apps, 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 District 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 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.

The following notice will be included as part of the computer log-on screen:

"District Technology Resources (as defined in Bylaw 0100) are to be used for educational and professional purposes only. Users are reminded that all use of District Technology Resources, including Internet use, is monitored by the District and individual users have no expectation of privacy."

Monitoring includes active attacks by authorized employees and/or agents of the School District to test or verify the security of the system. During monitoring, information may be examined, recorded, copied, and/or used for authorized purposes. All information, including personal information, placed on or sent over the system may be monitored. Such monitoring may result in the acquisition, recording, and/or analysis of all data communicated, transmitted, processed, or stored in this system by a user. Unauthorized or inappropriate use may subject you to disciplinary action and/or criminal prosecution. Evidence of unauthorized or improper use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this computer system, authorized or unauthorized, constitutes consent to monitoring for these purposes."

N. Use of the Internet and any information procured from the Internet is at the student's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or the services provided by or through District Technology Resources will be error-free or without defect. The Board 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 Board 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 Board is not to be responsible for financial obligations arising through the unauthorized use of its Technology Resources. Students or parents of students will indemnify and hold the Board harmless from any losses sustained as the result of a student's misuse of District Technology Resources.

O. 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."

P. Proprietary rights in the design of websites hosted on Board-owned or leased servers remains at all times with the Board.

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

R. Students may not use District Technology Resources to establish or access web-based e-mail accounts on commercial services (e.g., Gmail, iCloud, Outlook, Yahoo mail, etc.).

S. 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 District's users will be fully investigated and disciplinary action will be taken as appropriate.

T. Preservation of Resources and Priorities of Use: District 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 District Technology Resources for class- or instruction-related activities have priority over other users. Students not using District Technology Resources for class-related activities may be "bumped" by any student requiring access for class- or instruction-related purpose. The following hierarchy will prevail in governing access to District Technology ResourcesDistrict printers may only be used to print 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 District 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 Technology Manager.

Revised 10/09
Revised 2/18/15

Legal

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

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

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