Wayne County School District - Acceptable Use of Electronic Resources – Internet Safety

Revised: May 15, 2012. Approved: June 4, 2012

General:

The Wayne County Board of Education recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, the Wayne County School district will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology in schools. The district's technology will enable educators and students to better communicate, learn, share, collaborate, create, solve problems, and manage their work.

The Wayne County Board of Education will provide robust electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities, to develop procedures to support this policy, and to ensure the use of technology is consistent with the West Virginia Department of Education Policy 2460 – "Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet".

Purpose:

This policy is provided to ensure effective, safe, and appropriate use of electronic resources, technologies and the Internet. It is intended to promote and support positive digital citizenship among students and staff. While the district will make every reasonable attempt to provide a safe and effective digital environment, users must also share responsibility to maintain a safe environment.

Guidelines:

Network

The state and district networks (WANs) and school networks (LANs) include wired and wireless computers, servers, routers, switches, wireless access points, tablets, handheld devices and peripheral equipment, system files, user documents, Internet access and electronic communications, including email, messaging, blogs and wikis.

- All use of the network must be authorized by the school or district. Authentication will be provided through assigned login names and passwords. Temporary access for presenters or guests may be provided if appropriate and for the educational process.
- All use of the network must support instructional and/or administrative purposes and be consistent with WVDE and district policies and guidelines, E-Rate regulations and state and federal laws.
- All users must receive training on and accept all provisions of this Acceptable Use Policy in writing each year.
- Electronic filtering is employed by the WVDE at the two "Points of Presence" (POPs) to the Internet to prevent access to inappropriate material. Additional technologies and or methods may employed by the district to further protect users from inappropriate content.
- The WVDE and district reserve the right to prioritize the use of and access to the network.

Internet and Network Safety
No student should be allowed network or Internet access without the supervision of educator or staff member. Staff shall make every reasonable attempt to monitor students' activity while online.

Students and staff should not reveal personal information, including a home address and phone number, on blogs, podcasts, videos, wikis, email or web sites (unless required for specific registration purposes with prior administrative approval).

Students and staff should not reveal personal information about another individual on any electronic medium.

No student pictures or videos containing students or student names may be published on any class, school or district web site unless the appropriate permission has been verified according to district policy.

No student or staff member may assume another persons' identity while online.

Cyber Bullying is a serious matter and should be treated as such. Each student shall annually participate in the Internet Safety and Cyber Bullying lessons provided by the WVDE through the TechSteps program to comply with FCC and E-Rate regulations. Instructional information regarding the WVDE method and curriculum content for certifying that students have been educated about appropriate online behavior can be found at http://wvde.state.wv.us/technology/cipa-compliance.php.

Any student who participates in Cyber Bullying, inappropriate use or misuse will be subject to the disciplinary actions of this policy as well as WVDE Policy 4373.

If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Social Networking
Professional standards dictate that an adult should never be alone with a student in an isolated space (e.g., one student, one teacher together in a classroom with the door closed or after school operating hours). This is true in online environments as well. Social networking sites are structured to be closed environments, and as such the District discourages students and teachers from using social networking sites to communicate with one another. Secure and traceable communication tools are available for any school related communications between staff and students such as online grade book software or school email.

Confidentiality
All student educational data is protected by the Family Education and Privacy Act (FERPA) and other Federal and State laws. Disclosure of this data is strictly prohibited.

Privacy
The network is intended for use in the educational process of the district. Personal use should be kept to a minimum and never involve inappropriate material. There is no expectation of privacy to any individual on the network and the district reserves the right to monitor, review and store information about content and usage of the network. The district reserves the right to disclose any electronic file or message to law enforcement officials or third parties as appropriate for discovery, investigations or disciplinary action.

Student Use of Cellular Phones and Other Devices
The Board recognizes that many students possess cellular telephones and other electronic devices. These devices may not be used in any manner that disrupts the educational process, is illegal, or violates Board policies and/or school rules. Access to the network from these devices is prohibited without express permission from administration. Wayne County School District is not responsible for damage, loss or theft of such devices.

Staff Use of Cellular Phones
The Board recognizes that as adults, there are times that personal communications while at work are unavoidable. The Board also recognizes that many staff members possess cellular telephones making personal communication (phone and/or texting) much more convenient. Ringtones, vibrations, and other message acknowledgment methods as well as the communication itself can be distracting to the teaching and learning process in the classrooms. Personal communication during class time should be restricted to emergency situations only. Any business related communications should be kept to a minimum. All other personal communications should be limited to duty free time.

Devices Issued or Loaned to Students or Staff
- Technology devices may be loaned to students or staff members as an educational tool and may be used for purposes specifically authorized by school/district administration.
- Staff members or Students and their families are responsible for the proper care of any loaned device at all times, whether on or off school property, including the costs associated with repairing or replacing the device.
- If a device is lost, this must be reported to the school administrator immediately. If a device is stolen, a report should be made to the local police and building administrator immediately.
- The Board's policy and rules concerning computer and Internet use apply to use of all Board owned devices at any time or place, on or off school property. Students and staff members are responsible for obeying any additional rules concerning care of any device issued by school/district administration.
- Violation of policies or rules governing the use of these devices, or any careless use of a device may result in a device being confiscated and/or a student only being allowed to use the device under the direct supervision of school staff. The student or staff member may also be subject to disciplinary action for any violations of Board policies/procedures or school rules.
- The device may only be used by the student or staff member to whom it is assigned.
- All use of school-loaned devices by all persons must comply with the school's Computer Use Policy and Rules as well as this policy.

Privately-Owned Devices or Staff
- A student or staff member who wishes to use a privately-owned device to connect to the school network must complete a "Use of Privately-Owned Device" form. For students, the form must be signed by the student, his/her parent, the school technology coordinator, and a building administrator. For staff members the "Privately-Owned Device" form must be signed by the staff member, the school technology coordinator and building administrator. There must be an educational basis for any request (student or staff).
- The school technology coordinator will determine whether a privately-owned device meets the school's network requirements based on guidelines provided by the district technology director.

- Requests may be denied if it is determined that there is not a suitable educational basis for the request and/or if the demands on the school's network or staff would be unreasonable.
- The staff member or student is responsible for proper care of his/her privately-owned device, including any costs of repair, replacement or any modifications needed to use the device at school.
- Staff members nor students have an expectation of privacy in their use of a privately-owned device while at school. The school reserves the right to search a privately-owned device if there is reasonable suspicion that the staff member or student has violated Board policies, administrative procedures or school rules, or engaged in other misconduct while using the device.
- Violation of any Board policies, administrative procedures or school rules involving a privately-owned device may result in the revocation of the privilege of using the device at school, confiscation and/or disciplinary action.
- The school/district may confiscate any privately-owned device used by a staff member or student in a school without authorization as required by these rules. The contents of the device may be searched in accordance with applicable laws and policies.

WEB Publishing:
The district recognizes the educational benefits of publishing information on the Internet by staff and students. School websites should be in good taste, grammatically correct with active links and current content. School websites should refrain from including non-educational links or links that would imply advertising for a product or service. WVDE has provided domain names for each school at no cost and hosting can be provided at the school server. The district will not assume any costs for domain registration or hosting.

School and district websites must comply with all provisions of WVDE Policy 2460.

Use of Electronic Resources, Technologies and the Internet

Acceptable Use:
- Creation of files, documents, projects, videos, web pages, and electronic portfolios using network resources in conjunction with the educational process or administration thereof.
- Appropriate participation in school sponsored blogs, wikis, and monitored social networking sites or online groups.
- Online publication of original educational material including student work with proper parental permission. Outside sources must be cited appropriately.
- Staff use of network for incidental personal use within district or school guidelines.

Unacceptable Use:
- Use or transmission of any material in violation of any U.S., West Virginia, or local law or regulation. This includes but is not limited to copyrighted material, threatening, abusive, or obscene material or material protected by trade secrets.
- Use for commercial activity by for-profit entities or personal monetary gain.
- Any activity that would be in violation of C.I.P.A., C.O.P.P.A., of F.E.R.P.A.

Specific examples of unacceptable use include but are not limited to:

- Viewing, creating, accessing, uploading, downloading, storing, sending or distributing obscene, pornographic or sexually explicit materials.

- Downloading, uploading, and/or executing malicious software including malware, spyware, trojan horses, viruses, bots, or time bombs.
- Downloading or uploading of exceptionally large files which may compromise bandwidth availability.
- Sending mass emails that are considered SPAM.
- Use of another person's authentication credentials. (username/password)
- Use of another person's online account including but not limited to online grading programs, email, blogs, wikis, or assessment sites.
- Illegally accessing or attempting to access another person's data or personal system files, computers, networks, or information systems.
- Providing personal authentication credentials to another user to gain access to the network, computers, files, or accounts.
- Corrupting, destroying, deleting, or manipulating system data with malicious intent.
- Hacking, cracking or vandalizing hardware or software.
- Disclosing, using or disseminating personal, non-directory information regarding students.
- Cyber bullying, hate email, defamation, harassment, discriminatory jokes or comments. This may include off-site situations that can have an effect on the educational process of the district or school.
- Downloading, installing and/or executing non-educational gaming, audio files, video files, or other applications without express permission from the administration. This includes streamed or online files.
- Political campaigning or expression of opinions for or against a political candidate.
- Creating, sharing, or storing information that could endanger others (eg; drug manufacture, bomb making, etc.)
- Plagiarism or copyright infringement.
- Comments, photos, audio or video postings related to school students or personnel through use of off-site resources that have an adverse affect on the educational process.
- Connecting any unauthorized device or equipment to the network.
- Deliberate manipulation of network hardware or software or authentication process to bypass security and/or safety measures including proxies and unauthorized DNS servers.
- Vandalism of any kind to any equipment or content as part of the district/school network.

Disciplinary Action

All users of the district's electronic resources, technologies and the Internet are required to comply with the district's policies and procedures.

Violation of any of the conditions of use explained in this policy could be cause for disciplinary action, including suspension or expulsion from school, termination of employment, or suspension or revocation of network and computer access privileges as well as compensation for damages as a result of the violation.

Approved by the Wayne County Board of Education at the Regular Meeting June 4, 2012.