ACCEPTABLE USE OF ELECTRONIC RESOURCES

Electronic Resources-Instruction
The Vinton-Shellsburg Community Schools board of directors 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 Vinton-Shellsburg Community School district will use electronic resources as a powerful and compelling means for students to learn core subjects and apply skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals do in workplaces and other real-life settings. The district's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives.

Electronic Resources
These procedures are written to support the Electronic Resources Policy of the board of directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions. All school e-mail communication for personal reasons should be on a limited basis. School email is subject to review and expected to meet the high standards of morality and ethics. (ITS #8)

Network
The district network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the district.

Acceptable use of School or Personal networks by district students and staff includes:
- Creation of educational materials using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff and student use of the network for incidental personal use in accordance with all district policies and guidelines;
- Personal devices will follow all district technology guidelines; failure to comply will result in confiscation of the device for remainder of the day. Second offense will result in confiscation until parents/guardians have been notified to retrieve the device. Personal devices will only have access to the guest wireless network and will not be hard-wired without administrator approval.

Unacceptable network use by district students and staff includes but is not limited to:
- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;
- Downloading, installation and use of games, audio files video files or other applications (including shareware or freeware) without permission or approval from VS Staff members;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and/or other unauthorized changes to hardware, software, and monitoring tools;

- Unauthorized access to other district computers, networks and information systems;
- Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks.
- No tampering with hardware and software configurations.
- Information posted, sent or stored online that could endanger others, that has no classroom related purpose.
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material.
- Identity Theft
- Unauthorized access to other networks, computers, information systems outside of the district.

Consequences of violating the AUP is subject to a case by case basis and individual consequences will be determined by each building administrator.

The district is not responsible for lost, damaged, or stolen personal devices that are brought in outside of school. Students/parents are responsible for stolen computers based on a case by case basis where the student is found at fault for not properly securing the computer.

Internet Safety: Personal Information and Inappropriate Content
Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.

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

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

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

All school e-mail communication for personal reasons should be on a limited basis. School email is subject to review and expected to meet the high standards of morality and ethics. (ITS #8)

Filtering and Monitoring
Filtering software is used by the District to block or filter access to objectionable material. The determination of what constitutes “objectionable” material is a local decision.
- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district;
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively; and
- The use of personal network devices to bypass district filters will result in confiscation of device until parents can retrieve device. Additional offenses will be dealt with by building principal and or board of education.

Copyright
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 generally prohibited.

However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

Network Security and Privacy
Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- Do not use the "remember password" feature of Internet browsers; and
- Log off, if leaving the computer.

Student Data is Confidential
District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

Disciplinary Action
All users of the district's electronic resources are required to comply with the district's policy and procedures and agree to abide by the provisions set forth in the district's user agreement.
Violation of any of the conditions of use explained in the district's user agreement, Electronic Resources Policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges. Depending on the violation, board policies pertaining to harassment may also be applied.

___ I agree to the above district technology policies and guidelines.

_____ _____
Parent signature Student signature

To give district permission of the following please initial next to all that apply.
__ I give permission to the VSCSD to post pictures of my child on school sponsored media.
__ I give permission to the VSCSD to post my child's first name as a part of school sponsored media.
__ I give permission to the VSCSD to participate in Social Media networks sponsored by the school.
__ I give permission to the VSCSD to publish my students' work on school sponsored media.

(REVISED 7/13/17)