2022P
Instruction

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.

Use of District Technology

Informed Consent
Students will be informed of expectations for online behavior and use of district technology prior to logging-on to the district's network. Expectations for responsible computing will be reinforced by classroom teachers, teacher-librarians, and other school district staff.

Network
The district network includes wired and wireless computers, laptops/tablets 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 network use by district students and staff includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards 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 use of the network for incidental personal use in accordance with all district policies and guidelines;

Unacceptable network use by district students and staff includes but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind with the exception of job searches with the teacher's or supervisor's approval;
- 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 the Informational Technology Director;
- Support or opposition for ballot measures, candidates and any other political activity;

- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and 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;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed at the completion of any investigation that may come from such action.

The District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

Internet Safety/Citizenship Instruction

Personal Information and Inappropriate Content:

- Students and staff should not reveal personal information, including a home address and phone number, on websites, blogs, podcasts, videos, wikis, email 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.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision determined by the Assistant Superintendent for Learning and Teaching in consultation with staff and administration.

- 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;
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;

- 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; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

Internet Safety Instruction
All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber-bullying awareness and response.

- Age appropriate materials will be made available for use across grade levels.
- Training on online safety issues and materials implementation will be made available for administration, staff and families.

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.

Ownership of Work
All work completed by employees as part of their employment will be considered property of the district. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the district, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

Open Educational Resources
Teachers will consider recommendations from the OSPI Digital Learning Department to identify high-quality Open Educational Resources for instructional support. For advanced classes, teachers will consider recommendations from the Open Source Library developed by the Washington State Board for Community and Technical Colleges. Open Educational Resources used as the core materials for a class must follow the approval process for Instructional Materials as per District Policy/Procedure 2020.

Online curriculum used by students via the West Valley Virtual Academy
As per WAC 392-121-188 (10), online curriculum offered by online providers approved by OSPI is approved for use by students via the West Valley Virtual Academy. As per WAC, because the online provider has been approved by OSPI, no additional approval process is required.

Applications (Apps)
Applications purchased for personal accounts may be used for educational purposes but staff/students will not be reimbursed for any applications purchased for personal accounts. Applications purchased for school accounts must be pre-approved prior to purchase. Applications used as the core materials for a class must follow the approval process for Instructional Materials as per District Policy/Procedure 2020.

Network Security

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.

The following 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 user account password, keep it in a secure location;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock the screen, or log off, if leaving the computer.

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

No Expectation of Privacy
The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic messages to law enforcement officials or

third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers nightly – Monday through Friday. Refer to the district retention policy for specific records retention requirements.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policy and procedures. Failure to comply may result in disciplinary action including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Wireless Devices

Regarding district issued devices, students will follow the use of devices procedures Staff who are issued devices will follow procedures for proper care.

Wireless Device Returns and Fines

Individual school devices and accessories must be returned to the School Office by the student at the end of each school year. Students who graduate early, withdraw, are long-term suspended or expelled, or terminate enrollment within the West Valley School District for any other reason must return their individual school device on the date of termination.

If a student fails to return the device at the end of the school year or upon termination of enrollment within the West Valley School District, the student will pay the replacement cost of the device. Failure to return the device will result in referral to a collection agency or pay replacement cost.

Proper Care for the Wireless Device

Students are responsible for the general care of the device they have been issued by the school. Devices that are broken or fail to work properly must be taken to the school office for an evaluation of the equipment.

General Precautions:

- The device is district property and all users will follow the acceptable use policy for technology within the West Valley School District.
- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Cords and cables must be inserted carefully into the device to prevent damage.
- Devices must remain free of any writing, drawing, stickers, or labels that are not the property of the West Valley School District.
- Students are responsible for their device security; never leave in an unlocked locker, unlocked car, or any unsupervised area.
- Students are responsible for keeping their device's battery charged for school each day.

- Students are not allowed to remove or deface the district provided case and the device must be in the case at all times

Screen Care

- The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.
- Do not lean on the top of the device when it is closed.
- Do not place anything near the device that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Clean the screen with a soft, dry cloth or anti-static cloth.
- Do not bump the device against lockers, walls, car doors, floors, etc. as it will eventually break the screen.

Using the Wireless Device at School

Devices are intended for use at school each day. In addition to teacher expectations for device use, school messages, announcements, calendars and schedules may be accessed using the device. Students must be responsible to bring their device to all classes, unless specifically instructed not to do so by their teacher.

Loaning of Devices

- Loaner devices may be issued to students when they leave their device at home or is in need of repair.

Charging the device's Battery

- Devices must be brought to school each day in a fully charged condition. Students need to charge the devices by plugging them into an electrical wall outlet only. Do not charge the devices from a computer port.

Screensavers/Background Photos

- Inappropriate media may not be used as a screensaver or background photo.
- Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, and gang related symbols or pictures or other items that are disruptive to the education process may result in disciplinary actions.

Sound, Music, Games, or Programs

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Games are not allowed on the devices.
- The device is provided for educational purposes. Priority for the data storage on the device will be given to school district software/apps. User data and apps may be wiped clean with each district upgrade/sync.
- Any violation of these policies may result in disciplinary action.

Home Internet Access

- Students are allowed to connect to their home networks on their devices. However, the District Acceptable Use Policy must be followed while at home, while using a district owned device.

Network Connectivity

The West Valley School District makes no guarantee that their network will be up and running 100% of the time. In the case that the network is down, the District will not be responsible for lost or missing data.

Software on Devices

Originally Installed Software

- The software/apps originally installed by the West Valley Schools must remain on the device in usable condition and be easily accessible at all times. From time-to-time the district may add software applications for use in a particular course. Periodic checks of devices will be made to ensure that students have not removed required apps.

Additional Software

- The district's technology department will manage the applications on all student devices. Students are not permitted to connect and/or synchronize their devices to any computers.

Circumvention of Managed Settings

- Any attempts by students to circumvent any district management settings such as software restoration or jailbreaking will result in the confiscation of the device and disciplinary action.

Inspection

- Devices will be selected at random for inspection. Students must comply with the request to have the wireless device inspected.

Procedure for Re-loading Software

- If the device experiences technical difficulties or illegal software has been downloaded, the device will be reformatted to default settings. The school does not accept responsibility for the loss of any software or documents deleted due to a reformatting. In addition, this may result in confiscation of the device with usage allowed only during the school day.

Software Upgrades

- Upgraded versions of licensed software/apps will be available from time-to-time. Students may be required to check in their devices for periodic updates and syncing.

Responsibilities for the Use of the Wireless Device

Parent/Guardian Responsibilities

- Talk to your children about values and the standards they should follow on the use of the Internet just as you do on the use of all media information sources such as television, telephone, movies, and radio.

School Responsibilities

- Provide access to the Internet
- Provide Internet blocking of inappropriate materials as able.
- Provide staff guidance to aid students in doing research and help assure student compliance for acceptable use.

Students Responsibilities

- Use devices in a responsible and ethical manner.
- Obey general school rules concerning behavior and communication that applies to laptop/table.
- Use all technology resources in an appropriate manner so as to not damage school equipment. This damage includes, but is not limited to, physical damage and the loss of data or service interruptions. Help the West Valley School District protect our computer system/device by contacting an administrator about any security problems they may encounter.
- Turn off and secure their device after they are done working to protect their work and information.
- Return their device to the School Office at the end of each school year. Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment for any other reason must return their individual school device on the date of termination.

Student Activities Strictly Prohibited:

- Illegal installation or transmission of copyrighted materials.
- Any action that violates existing Board policy or public law.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
- Use of chat rooms, sites selling term papers, book reports and other forms of student work.
- Messaging services – ex: MSN Messenger, ICQ etc. (Apple Messenger, Facebook Messenger).
- Unauthorized Internet/Computer Games.
- Use of outside data disks or external attachments without prior approval from the administration.

- Changing of device settings (exceptions include personal settings such as font size, brightness, etc.).
- Restoring or jailbreaking device.
- Connecting device to a computer and/or synchronizing device to a personal account.
- Downloading unauthorized apps.
- Spamming-Sending mass or inappropriate emails.
- Gaining access to other student's accounts, files, and/or data.
- Exchanging devices and/or switching device identification labels to conceal fault of damage.
- Use of the school's internet/email accounts for financial or commercial gain or for any illegal activity.
- Use of anonymous and/or false communications such as MSN Messenger, Yahoo Messenger.
- Students are not allowed to give out personal information, for any reason, over the Internet. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms, eBay, email, etc.
- Participation in credit card fraud, electronic forgery or other forms of illegal behavior.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients.
- Bypassing the West Valley Web filter through a web proxy.

Replacement or repair of a damaged or lost wireless device

Lost or Stolen Devices

- All lost or stolen devices must be reported to the school office.

Damaged Devices

- All damaged devices must be reported to the school office. Students/parents will be held responsible for ALL repairs to their device including, but not limited to: broken screens, cracked plastic pieces, inoperability from jailbreaking *cases*, cables, etc. All damaged devices must be repaired by the district.

Adoption Date: 06.01

Revised Dates: 06.08; 10.08; 07.13; 9.13; 08.16; 02.18