

EVSD NETWORK AND INTERNET USER AGREEMENT

*Network and internet misuse will incur disciplinary action relevant to the measure of the violation.

The East Valley School District 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. Advances in telecommunication technologies continue to change the way we communicate. From offices, schools, and homes we are able to travel electronically all over the world to gather information. As more people travel this electronic highway and use the ever growing variety of technologies and services becoming available, maps to find information and rules to keep users safe and accountable become vital to successfully completing the journey.

Therefore, the East Valley 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 for important purposes in schools just as individuals 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.

The Board directs the Superintendent or designee to create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities and to develop procedures to support this policy.

Acceptable Use Guidelines

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.

For the purpose of this Acceptable Use Policy, Electronic Resources is defined as the sending and receiving of electronic, analog or digital information using any school district equipment, systems or networks; including, but not limited to, computers, telephones, (wired, cellular, wi-fi), fax machines, local/wide/metropolitan-area networks, the district intranet, e-mail, voice-mail and the public internet.

East Valley School District's Educational Network and the Public Internet

The internet is a global network made up of many contributing networks that support the open exchange of information among many different kinds of institutions all over the world. The purpose of the East Valley School District's Educational Network and all of its technologies is to support the curricular needs and teaching and learning requirements of the district's educational program and to support the business and administrative needs of the school district's operations. Use of the East Valley school District's Educational Network and all of its technologies is a necessary element of the district's educational mission and business and administrative needs, and is furnished to staff and students as a privilege, not a right or entitlement. The district seeks to protect legitimate users of such technology by establishing guidelines for such use and imposing discipline on those who abuse the privilege.

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.

Filtering

The district will make every reasonable attempt to limit access to inappropriate material by using an internet filtering system, providing staff training, and encouraging personal responsibility and accountability. 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). 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. The user is ultimately responsible for his/her actions in accessing and using network services.

Appropriate Use of Computers, Technology and Network Resources

Student and staff use of district technology, computing and network resources must be in accordance with the educational and operational needs and objectives of the East Valley School District. This includes, but is not limited to, the following:

- Creation and storage of files, projects, videos, web pages and podcasts using network resources in support of the educational or operational needs of staff and students.
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;
- Participation in chat areas, instant messaging services, news groups, blogs, podcasts, RSS feeds, wikis, emails or other communication methods shall be permitted when used in conjunction with the curricular, educational or operational needs of staff and students.
- The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff electronic mail is subject to the same records retention rules that apply to other documents and must be retained in accordance with the retention schedules as indicated in policy #6570.

- Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable network use

This list includes, but is not limited to:

- Any use for individual profit or gain; for product advertisement; support or opposition for ballot measures, candidates and any other political activity; or for excessive personal use;
- Hacking, cracking, vandalizing, use of keyloggers, intentionally disrupting network traffic, the introduction of viruses, worms, Trojan Horses, time bombs and changes to hardware, software, and monitoring tools;
- Attempting to defeat or bypass the district's internet filter by using or trying to use proxies, https, special ports, modification to district browser settings or any other techniques designed to avoid being blocked from inappropriate content or to conceal internet activity;
- Attempting to defeat, disable or bypass any security protocols, authentication services, firewalls, PC or server system security settings or parameters, network intrusion detections services or any other technology that manages and secures the network;
- Cyberbullying, 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 manufacture);
- Unauthorized downloading or installation of any software, including shareware, freeware, and games;
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material;

Internet Safety

- Students and staff should not reveal personal information, including 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.
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

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.

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;
- Lock the screen, or log off, if leaving the computer.

Student data is kept confidential

District staff must maintain the confidentiality of student data in accordance with the Family Education 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 message to law enforcement officials or third parties as appropriate. Backup is made of all district staff e-mail for purposes of disaster recovery and public disclosure. All documents are subject to the public records disclosure laws of the State of Washington.

Disclaimer

East Valley School District makes no warranties of any kind, whether express or implied, for the computing and network services it provides and is not responsible for material viewed or downloaded from the internet by users. Use of any information obtained via the internet is at the user's own risk. Users must be aware that there are many services available via the internet that might be offensive to certain groups of users. East Valley School District has filters and security in place to block staff and student access to inappropriate and/or offensive material available via the internet but these filters are not a guarantee that all inappropriate material is blocked. East Valley School District cannot eliminate access to all such services, nor could the district begin to identify all of them. Individual users are responsible for their own actions in navigating the internet using East Valley School District technology resources.

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.

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 East Valley School District's network use agreement. Unethical and unacceptable behaviors, inappropriate use of district computers, systems, networks and technology resources, and any violation of this Acceptable Use Policy shall be cause for taking disciplinary measures against staff in accordance with district policy, collective bargaining provisions, and against students consistent with Policy 3200, Student Rights and Responsibilities.