

3.18 – TECHNOLOGY ACCEPTABLE USE

GENERAL

Philosophy

The Van Buren School District (VBSD) is committed to using the latest technology available to promote educational excellence by facilitating resource sharing, innovation, and communication. Technology should be readily available in the classroom and should be used as a tool to make opportunities available for all students and staff to maximize their potential.

Internet

Internet access is coordinated through a complex association of government agencies and regional and state networks. The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. VBSD is connected to the Internet through the Arkansas Public School Computer Network (APSCN). APSCN was formed in 1993 in order to link every public school educational cooperative, and the Arkansas Department of Education.

Internet Safety

The on-line world, like the rest of society, is made up of a wide variety of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or mean and exploitive. Access to the Internet is free of charge and available to all students with valid accounts regardless of gender, age, ethnic background, or religious beliefs.

Congress passed the Children's Internet Protection Act (CIPA) which requires schools and public libraries that access certain federal funds to equip all computers that might be used by students with a system to block sites that are obscene or show material harmful to minors. Required classes will be held yearly for educating minors about appropriate online behavior, including but not limited to interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response. The state of Arkansas has also passed legislation requiring school districts to provide Acceptable Use Policies which are signed by students, to provide filtered Internet, and to provide online safety classes. The Van Buren School District receives Internet access from the Arkansas Public School Computer Network (APSCN), and VBSD provides the Internet Filtering to meet CIPA compliance.

Acceptable Use

Each user is expected to use accounts responsibly, with purposes for which such accounts are granted. Activities beyond these stated purposes are strictly prohibited and may result in restricted or revoked access to computing resources.

Users of computer software owned by VBSD must agree to abide by the limitations included in the copyright and license agreements entered into with vendors. Furthermore, it is the user's responsibility to become familiar with the specific copyright and licensing agreements for each product before using it. It is unlawful to copy most software products. If other arrangements are made with a vendor, users must abide by the stated provisions. VBSD has many resources of an instructional entertainment nature, which are available to students. Users working on educational projects, however, always have priority when it comes to using the computers.

Unacceptable Use (Including but Not Limited to the Following)

Users shall not attempt to access, copy, or destroy programs or files that belong to other users or to VBSD

without prior authorization. Programs, subroutines, and data provided by VBSD may not be taken to other computer sites without authorization. Also, programs acquired at other computer sites must not be used at VBSD unless permission to use them at VBSD is granted.

No user is permitted to install software or change the configuration on computers without ~~written~~ consent from the District Technology Staff (DTS).

- Purchase of computers should be reviewed and approved by the DTS.
- Teachers and Administrators: Please do not install software unless it has been approved by the DTS.
- Administrators: the best practice for purchasing school site software is to have a member of the DTS review and approve the software before purchase. If you need software placed on your computer, please complete a helpdesk ticket.

Users should minimize the impact of their work upon the work of others. One should not encroach on others' use of the facilities or deprive them of system resources. **Users shall not attempt to modify system facilities in any way** Intentional compromise of system integrity by virus or other means is a serious offense. Staff should always login to the network with their correct login and store their files inside their "Documents" location on the server to ensure backup. Machines should be turned off after proper log off each day. The district technology staff will not attempt to recover files which are not backed up.

Users shall not subvert restrictions associated with their accounts. The list below does not cover every situation that pertains to proper or improper use of the computing resources on VBSD, but it does suggest some of the responsibilities that you accept if you choose to use a VBSD computer. Disciplinary action will be taken whenever any user is found to be in violation of the responsible use of the computers or network.

- Revealing personal address or phone numbers or those of other students or colleagues
- Violating the rights of privacy of students and employees
- Using profanity, obscenity or other language which may be offensive to another user
- Using the network illegally in ways that violate federal, state, or local laws or statutes
- Reporting personal communications without the author's prior consent
- Using the network for financial gain or for any commercial or illegal activity
- Using the network to send or retrieve pornographic material, inappropriate text files, or files dangerous to the integrity of the network
- Spreading computer viruses, or in any way causing disruption of the network, such as sending large e-mail files, etc.
- Downloading, storing or printing files or messages that are profane, obscene, or that use language that offends or tends to degrade others
- Product advertisement or political lobbying
- Circumventing security measures on school or remote computers or networks
- Attempting to gain access to another's resources, programs, or data
- Falsifying one's identity
- Changing any computer files that do not belong to the user
- Failure to use disk storage space wisely and efficiently - (delete unnecessary e-mails and files)
- Copying files without permission to local hard drives or network drives especially audio files and movie files.
- Misuse or vandalism of equipment
- Communicating credit card numbers, or any other financial information - (personal online banking on school computers is highly discouraged for your own security)
- Gaining unauthorized access to resources or entities
- Posting anonymous messages

- Violating copyright restrictions (which are the same as for printed materials)

STUDENTS

E-mail

As a general rule, VBSD does not provide e-mail accounts to students. Personal e-mail should be accessed at home not school. If need can be shown that a student account is necessary they should present that need to the principal for written approval. E-mail should then only be accessed under supervision. At that point the student should understand that anything written on e-mail is public information.

Penalties for Improper Network Use

Use of public property for personal gain is a felony and is subject to prosecution.

- | | |
|------------|---|
| Classroom: | Classroom violations of this policy may result in loss of privileges and/or disciplinary action. |
| District: | Suspension or cancellation of VBSD network privileges and/or disciplinary action. State: Applicable state laws apply. |
| Federal: | Applicable federal laws apply. |

PARENTS

Guidelines for Parents

- Never give out identifying information such as home address, school name, or telephone number in a public message such as chat or bulletin boards, and be sure you are dealing with someone that both you and your children know and trust before giving out any information through electronic messages.
- Get to know the services your child uses.
- Never allow a child to arrange a face-to-face meeting with another computer user without parental permission.
- Never respond to messages or items that are suggestive or make you uncomfortable in any way.
- Report suspicion of child pornography to National Center for Missing Exploited Children at 1-800-843-5678.
- Remember that people on-line may not be who they seem.
- Remember that everything you read on-line may not be true.
- Establish and enforce reasonable rules and guidelines for computer and/or "on-line" use by your children.
- Make it a family activity. Get to know their on-line friends just as you know their other friends.

Letter To Parents

Your child has requested access to the VBSD Network. The school district is able to offer network access to all students who agree to abide by the acceptable use policies, sign a contract, and have parent permission.

Access to the network will provide your child with access to the Internet. It is possible that your child may run across areas of adult content and some material that you might find objectionable. While we do not encourage access to such material, it is not possible to block access to all such sites, even though every effort to filter such content has been provided through our state system.

In some classes, students will also have the opportunity to design their own web page which could include information about themselves (including pictures) and links to other sites. Students are cautioned about displaying personal information. Open communication with your children, utilization of such computer resources, and getting on-line yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use.

Part of the school district's responsibility in preparing our students for the 21st century is to provide them access to the tools they will be using in postsecondary education and in the work place. We believe that the use of this global information network is one of those tools. The school district will provide training in using the network and endeavor to teach students their responsibility as network citizens and guidelines for ethical conduct in this new global community.

FACULTY/STAFF

E-mail

Personal use of electronic mail is permitted within reason. Sending unprofessional or unethical messages or messages deemed to be disruptive to the education process is in violation of Acceptable Use Guidelines. Personal use should be kept to a minimum. Users are not permitted to conduct a business using any school technology resources. Note: e-mail is not private. The DTS have access to all mail and may read mail if justifiable reasons exist to do so. Users should also be aware that e-mail can be traced to the sender and can be monitored for unacceptable language or inappropriate use. E-mail is backed up. Individuals are responsible for e-mail left on their computers. Do not use distribution lists to send messages to staff unless there is an educational reason to do so. You should consider e-mail received or sent at school as a matter of public record. Remember, if you would not write it in a letter or postcard, do not write it in e-mail or e-mail attachments.

Internet

Internet service is provided by Arkansas Public School Computer Network (APSCN). It is to be used for educational purposes. Using the Internet for personal use must be kept to a minimum in order to provide the bandwidth needed for everyone to use. This includes but not limited to peer-to-peer file sharing programs, chat programs, internet radio, internet video clips, and public bulletin boards. Accessing these things is a security risk and denies bandwidth for legitimate use. All internet traffic can and will be monitored.

Security

Do not allow students to use your account. Do not store your passwords in your desk or where they are easily available. Your billfold or purse, wherever you keep your driver's license or credit cards, is the best place to keep passwords.

Backup your important files to a network location where they are secure and backed up with the servers in case of disaster recovery. If something happens to your computer, it will be much easier to repair if you have saved all your files to the designated location. The DTS is not responsible for backing up individual data not stored on servers.

Computers

Computers belong to the school district and must be treated accordingly. They are to be used for educational purposes. Software should not be installed or changes made unless you inform the DTS.

Do not set system passwords DTS. User passwords may be changed as desired. Screen savers, Web Shots, Comet Cursor, and other freeware or shareware should not be installed. Numerous problems have resulted from the use of such software. DTS will not be responsible for problems which occur as a result of installing such software.

Penalties for Improper Use

Problems will be reported to the building principal and/or the appropriate local, state and federal authorities.

Reporting Problems

DTS is trying to cut response time for problems. Please use the system DTS has in place for requesting service. Service request forms are submitted through the online helpdesk on the district website. Priority is given to network problems, computer labs, food services, and administration/faculty/staff. If you have an emergency, please call or leave a message at 471-3113.

Virus Protection

Virus protection has been added to all network computers in an effort to cut down on problems. Please do not open attachments unless you know what they are. Some of the new viruses are very destructive. It is much easier to check with the sender to verify the e-mail than to redo your computer. Do not attempt to alter or remove the anti-virus program. If you are notified of a potential virus threat please forward it immediately to technology@vbsd.us - DO NOT DISTRIBUTE THE VIRUS WARNING ON A DISTRICT LEVEL.

Purchasing

The purchase of computers or software should be cleared through DTS. Call or e-mail the Director in the technology department. It is very important that we coordinate our efforts in order to provide the best service to staff, students, and parents. We can also assist in obtaining the best prices for goods and services.

APPLICABLE LAWS

Family Educational Rights and Privacy Act (FERPA)

Public information, such as student photos cannot be published on the Internet, unless: the school is otherwise notified in writing from a parent

Children's Internet Protection Act (CIPA)

House Bill 2503-Act 1747

Requires districts to publish certain items on district web pages, and provide policy regarding the Internet with penalties for violations.

Responsibilities of Employees on Internet Act 1287 of 2001 AUP
American Disabilities Act

Approved by Board: March 14, 2006
Amended by Board: May 10, 2011
Amended by Board: Feb 7th, 2012