VALLEY STREAM UNION FREE SCHOOL DISTRICT TWENTY FOUR

COMPUTER RESOURCES AND DATA MANAGEMENT **Policy 6165**

The Board of Education recognizes that computers are a powerful and valuable education and research tool and as such are an important part of the instructional program and that it is critical to exercise appropriate control over computer records, including financial, personnel and student information.

This policy covers all users of computers and other technology that may provide access to the Internet and/or other networks within or linked with the School District (the School District's "computer resources"). Computer resources provide the School District, its personnel and students with unique opportunities for the sharing of knowledge, information and ideas that can positively impact on the instructional and organizational programs. With access to the School District's computer resources comes the responsibility for proper on-line conduct, acceptable use of the network, proper use of copyrighted material, and sanctions for inappropriate use.

General Provisions

The Superintendent of Schools or his/her designee shall be responsible for designating an individual(s) who will oversee the procurement and use of the School District's computer resources. Said individual will prepare in-service programs for the training and development of School District staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas.

All users of the School District's computer resources must understand that use is a privilege, not a right, and that use entails responsibility. Users of the School District's computer resources must not expect, nor does the School District guarantee, privacy for electronic mail (e-mail) or any use of the School District's computer resources. The School District reserves the right to access and view any material stored on School District equipment or any material used in conjunction with the School District's computer resources.

Use of the Internet

- All use of the network or other on-line servers must be in support of education and research or administration/management consistent with the goals of the School District.
- Any use of the School District's computer resources for private, commercial and political business is prohibited.
- Any use of the School District's computer resources for profit is prohibited.
- Any use of the School District's computer resources for information that is deemed by the supervising staff member and/or school administration to be dangerous, objectionable, pornographic, distracting and/or otherwise offensive in nature is prohibited.
- Users of the School District's computer resources are not to intentionally seek information about other users that could be private in nature.
- The malicious use of School District's computer resources is prohibited.

- Electronic hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited.
- Users of the School District's computer resources shall use only the passwords assigned to themselves and not seek to misrepresent themselves as other users.

Unauthorized tampering or mechanical alteration including software configurations will be considered vandalism, which is prohibited and illegal.

School District Limitation of Liability

The School District makes no warranties of any kind, express or implied, that the functions or the services provided by or through School District's computer resources will be error-free or without defect. The School District will not be responsible for any damage users may suffer including but not limited to, loss of data or interruptions of service. The School District is not responsible for financial obligations arising through the unauthorized use of the School District's computer resources.

Account Access to Network, E-Mail Accounts and Computer Services

1. All student users of the School District's computer resources will have access according to his/her assigned rights. Approved class work shall have priority over other uses. No single user should monopolize a computer, unless specifically assigned for special needs.

2. All use of the School District's computer resources must be in support of education and research or administration/management consistent with the goals of the School District. The term "education" includes use of the system for classroom, professional or career development activities.

3. Users are responsible for the use of his/her individual account and should take all reasonable precautions to prevent others from being able to access their account. The user will be held responsible for any policy violations that are traced to their account. Under no conditions should a user provide his/her password to another person.

4. Users may be required to remove files if School District's computer resources storage space becomes low.

5. Users who are provided a School District email address will check his/her e-mail on a regular basis and delete unwanted messages promptly.

6. School District administrators have the right to access e-mail to investigate complaints. Any violations of the acceptable use policy will be reported to appropriate personnel.

7. The use of group forums, including "chat rooms," is only permitted when used for an educational purpose.

System Security

1. Software shall be installed by authorized School District computer administration personnel only.
2. The permission of the Superintendent of Schools or his/her designee is necessary in order to download or install software.
3. Permission of the Superintendent of Schools or his/her designee is required for the relocation, removal or adjustment of any hardware and/or peripheral device.
4. Food and/or drink shall not be placed in the immediate area where computers are located.
5. Passwords must be changed every one hundred twenty (120) days, except for passwords associated with the School District's financial software (which passwords will be changed every 90 days). Passwords must be at least eight (8) and not more than fourteen (14) characters in length and must contain at least one (1) uppercase letter, one (1) lowercase letter, and one (1) number/special character, except for passwords associated with the School District's financial software (which passwords must be at least six (6) characters in length and must contain at least one letter, one number and one special character). Passwords shall not contain:

    a. Common acronyms,
    b. common words or reverse spelling of words,
    c. names of people or places,
    d. any part of the login name;
    e. numbers easily remembered such as phone numbers,
    f. social security numbers, and/or
    g. street addresses.

In addition:

    a. All passwords shall be secured by the individual and not shared with others.
    b. Passwords should not be written down;
    c. Passwords shall not be sent via email to anyone; and
    d. Individuals shall not use the "Remember Password" feature of any application or program.

6. All users are required to log out or lock their computers when the computer is unattended.

Controls for Financial Computer Software Applications

1. In connection with the operation and maintenance of the School District's financial software product, the Superintendent of Schools shall not serve any business function beyond that of administration of the School District's financial networking.
2. Approval for change of permissions on the School District's computer resources related to the School District financial software product must be submitted to the Assistant Superintendent for Business for approval. Once the Assistant Superintendent for Business has approved the request for a change of permissions, the request will be sent to the Superintendent of Schools for approval. No change in permissions will be granted in the absence of said approvals.
3. The School District's accounting and financial data will be backed up daily. A back up of such data will be maintained offsite and shall be maintained regularly by the Superintendent of Schools. In addition, the School District will develop a disaster recovery plan in the event of catastrophic loss.
4. Segregation of duties in the computer system for financial affairs will be consistent with the manual system. Thus, electronic permissions of employees should appropriately reflect their duties. The School District administration will also implement appropriate controls when adequate segregation of duties is not practical or possible.
5. In connection with remote access to the School District's financial management system, remote access shall only be permitted by the financial software vendor for purpose of updating the system. This access must be pre-approved by the Superintendent of Schools or his/her designee.
6. Passwords for all financial network facilities must be changed every ninety (90) day. All passwords must be at least six (6) characters in length and must contain at least one letter, one number and one special character.
7. The system administrator should be physically located outside of the business office and have no business function. The role of the systems administrator should be to change an electronic permission when a request is made and approved as set forth above.

<u>Plagiarism and Copyright Infringement</u>

a. Any software that is protected under copyright laws will not be loaded onto or transmitted via the network or other on-line servers without the prior written consent of the copyright holder.
b. Users will honor all copyright rules and not plagiarize or use copyrighted information without permission. Plagiarism is the use of writings or ideas of others and presenting them as if they were the creation of the presenter.

c. The School District will receive written permission from parents and/or guardians prior to publishing any student's work on the Internet or School District web pages.

Illegal Activities

a. Users will not knowingly or recklessly post false or defamatory information about a person or organization.
b. Attempts to log on through another person's account or to access another person's files is illegal and this conduct shall not be engaged in except that the School District's administrators shall have the right to log on through another person's account and access another person's files as provided for in this policy or for network security reasons.
c. Any use of the School District's computer resources for profit is prohibited.
d. Any use of the School District's computer resources for information that is deemed by the supervising staff member and/or school administration to be dangerous, objectionable, pornographic, distracting to education, or otherwise offensive in nature is prohibited.
e. Users will not post chain letters or send messages to large numbers of people.
f. Electronic hate mail, harassment, discriminatory remarks, inappropriate language, cyberbullying and other illegal and/or antisocial behaviors are prohibited.
g. Users of the School District's computer resources shall only use their assigned passwords and not seek to misrepresent themselves as other users.
h. Users may not use the School District's computer resources to engage in any illegal act, such as arranging for a drug sale, purchasing alcohol, engaging in criminal activity, threatening the safety of a person, etc.
i. Unauthorized exploration of the network operating system or unauthorized changes to any installed software is strictly prohibited.
j. Any use of the School District's computer resources for the purpose of gambling is prohibited.

Personal Use

a. Users may not use the School District's computer resources for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. School District acquisition policies will be followed through the School District's computer resources.
b. Users may not use the School District's computer resources for political lobbying in support of or in opposition to individual candidates seeking election or political parties.

c. Users may not post personal information about themselves or others, such as their last name, home address, work address, phone number, school name or address.
d. Users will not transmit pictures of themselves or other people unless in conjunction with authorized school use.

Respect for Privacy

a. Users are not to intentionally seek information about other users that could be private in nature.
b. Users will not post private information about another person.

Vandalism

a. Any act of vandalism is strictly prohibited. Vandalism is the malicious attempt to destroy or harm data or equipment.
b. Uploading, creating or spreading computer viruses is considered to be an act of vandalism.

Access to Inappropriate Material

a. Users will not utilize the School District's computer resources to access material that is profane or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people.
b. The user should, as soon as practical, report any inadvertent incident in a manner specified by their school. This will protect them against an allegation that they have intentionally violated the acceptable use policy.

Consequences

Unacceptable uses of the School District's computer resources may result in the suspension or cancellation of computer privileges, as well as disciplinary, monetary, and/or legal consequences.

Technology and Instruction

Teachers are encouraged to use technology to improve student achievement. Portable storage devices such as flash drives and discs with files will be permitted in the interest of enhancing instruction.

In addition, the Superintendent of Schools or his/her designee will develop procedures which address:

- system administration
- separation of duties

- data back-up (including archiving of e-mail)
- record retention and
- disaster recovery plans.

Review and Dissemination

This policy will be reviewed on a regular basis by the Board of Education.

Cross Ref**:** 6166 Computer, Network and Internet Acceptable Use
6167 Internet Safety
6168 Information Security Breach and Notification

Adoption Date: June 12, 2019