606.06R2 Staff use of Computers, Technology and the Internet

Friday, August 11, 2023

STAFF USE OF COMPUTERS, TECHNOLOGY AND THE INTENET

Acceptable Use

The use of computers, technology and the Internet must be consistent with the educational objectives of the School District. All School District electronic resources must be used in a responsible, efficient, ethical and legal manner. Failure to adhere to these regulations will result in loss of user privileges, disciplinary action, dismissal and/or appropriate legal action.

Privileges

The use of the District's electronic networks is a privilege, not a right. The Building Principal will make all decisions regarding whether or not a user has violated this authorization and may deny, revoke, or suspend access at any time.

Unacceptable Use

The user is responsible for his or her actions and activities involving electric resources. Some examples of unacceptable uses are:

1. Using the network for -*any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law.

2. Unauthorized loading or downloading of software, games or files, regardless of whether they are copyrighted or devirused.

3. Downloading copyrighted material for other than personal use.

4. Commercial or for-profit uses.

5. Wastefully using resources, such as file space.

6. Destroying, modifying or abusing hardware or software.

7. Gaining unauthorized access to resources, files, passwords or other users' accounts.

8. Accessing the Internet from a School District access point using a non-school district Internet account.

9. Accessing fee services via district technology without specific permission from the Building Principal.

10. Accessing, receiving, transmitting or re-transmitting material regarding students, parents/guardians or district employees that is protected by confidentiality laws. If material is not legally protected but is of a confidential or sensitive nature, great care shall be taken to ensure that only those with a "need to know" are allowed access to the material. Staff members shall handle all employee and student records in accordance with School District policies and regulations.

11. Invading the privacy of individuals.

12. Disrupting the work of others.

13. Posting material authorized or created by another without his/her consent.

14. Impersonation of another user, anonymity and pseudonyms.

15. Sending or accessing encrypted information.

16. Commercial or private advertising, or political lobbying.

17. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, discriminatory, offensive, harassing, or illegal material.

18. Using or attempting to use the resources while access privileges are suspended or revoked.

No Expectation of Privacy

Use of the District's electronic resources, including e-mail, is not private. The District reserves the right to log, monitor, examine, evaluate, and disclose solely at its discretion, the contents of all files, communications, or other usage on or conducted through these resources despite any designation of privacy by either the sender or recipient.

No Warranties

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the users' errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification

The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security

Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify appropriate personnel. Do not demonstrate the problem to other users. Users shall not reveal their passwords to other individuals. Attempts to logon to the Network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to these resources.

Vandalism

Vandalism will result in cancellation of privileges and will be reported to the legal authorities for possible prosecution. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Telephone Charges

The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Limited Resource

Activities that are deemed by the network supervisor to cause unreasonable demand on network capacity or disruption of system operation are prohibited. Users shall not post chain letters or engage in "spamming". Spamming is sending unsolicited messages to a large number of people, or sending a large number of unsolicited messages to one or a few individuals.