Valley View School District 365U Acceptable Use Policy

Authorization for Computer Network and Internet Access

All use of Valley View School District network resources, including the Internet, shall be consistent with the District’s goal of promoting excellence by facilitating resource sharing, innovation and communication. The purpose of this network is to assist in preparing users for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. This Authorization does not attempt to state all required or proscribed behavior by users.

Terms and Conditions

Acceptable Use

- Access to the District’s network resources, including the Internet, must be for the purpose of education or research, and be consistent with the educational objectives of the district. Transmission of any material in violation of United States or state statute or regulation is strictly prohibited. This includes but is not limited to copyright or trade secret material, threatening or obscene material, and criminal activity. The use of the network resources for commercial activities, product solicitations, or political lobbying is also prohibited. Inappropriate use will be reported to the responsible authorities.

Some examples of unacceptable behaviors are:

- 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.
- Unauthorized installation of software.
- Engaging in personal attacks, including prejudicial or discriminatory attacks.
- Harassing another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages, they must stop.
- Downloading copyrighted material for other than personal use.
- Using the network for private financial or commercial gain.
- Wastefully using resources, such as file space.
- Gaining unauthorized access to resources or entities.
- Invading the privacy of individuals.
- Using another user’s account or password.
- Posting material authorized or created by another without his/her consent.
- Posting anonymous messages.
- Using the network for commercial or private advertising.
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, or illegal material.
- Using the network while access privileges are suspended or revoked.
- The taking, disseminating, transferring, or sharing of obscene, pornographic, lewd, or otherwise illegal image or photographs, whether by electronic data transfer or otherwise (commonly called texting, sexting, emailing, etc.) may constitute a CRIME under state and/or federal law. Any person identified as taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images or photographs may be subject to arrest, criminal prosecution, and LIFETIME inclusion on sexual offender registries.

Privilege

- The use of the District's network resources, including the Internet, is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The appropriate building or district administrator will make decisions regarding whether or not a user has violated the Authorization. A copy of network etiquette and unacceptable uses can be found in the student handbook.
System Security

- Users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them. Under no conditions should users provide their password to another person.
- Users must immediately notify a building administrator and/or the technology department if they have identified a possible security problem. Users should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Users will not attempt to gain unauthorized access to any portion of the Valley View School District electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing”.
- Users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Users will not attempt to access Web sites blocked by district policy, including the use of proxy services, software, or Web sites.
- Users will not use sniffing or remote access technology to monitor the network or other user’s activity.

No Warranties

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

Violations of this Acceptable Use Policy

Violations of this policy may result in loss of access as well as other disciplinary or legal action. Violation of this policy shall be subject to the consequences as indicated within this policy as well as other appropriate discipline, which includes but is not limited to:

- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension and/or expulsion from school
- Inspect or review accounts and files for security purposes
- Legal action and prosecution by local law enforcement and/or other appropriate state or federal agencies

The particular consequences for violations of this policy shall be determined by the school administrators. The superintendent or designee and the board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.