

Van Alstyne ISD - Acceptable Use Policy

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(REGULATION)

The Superintendent or designee will oversee the District's electronic communications system.

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner (s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent) or employee who created the work. [See CQ (EXHIBIT)]

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Education Records Privacy Act and District policy. [See CQ(EXHIBIT) and policies at FL]

SYSTEM ACCESS Access to the District's electronic communications system will be governed as follows:

1. As appropriate and with the written approval of the immediate supervisor, District employees will be granted access to the District's system.
 - o 2. Students in grades PreK – 12 will be granted access to the District's system by their teachers, as appropriate. Students participating in computer courses will be assigned individual accounts.
3. The District will require that all passwords be changed every 60 days.
4. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.

TECHNOLOGY COORDINATOR RESPONSIBILITIES The technology coordinator for the District's electronic communications system (or campus designee) will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or supervisor's office.
3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.
6. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
7. Set limits for data storage within the District's system, as needed.

INDIVIDUAL USER RESPONSIBILITIES The following standards will apply to all users of the District's electronic information/communications systems:

ON-LINE
CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
4. Students may not distribute personal information about themselves or others by means of the electronic communication system.
5. System users must purge electronic mail in accordance with established retention guidelines.
6. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
7. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may noncommercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.
8. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
9. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
10. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
11. System users may not waste District resources related to the electronic communications system.
12. System users may not gain unauthorized access to resources or information.

**VANDALISM
PROHIBITED**

Any malicious attempt to harm or destroy District equipment or data or data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct]

**FORGERY
PROHIBITED**

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

**INFORMATION
CONTENT / THIRD-
PARTY SUPPLIED
INFORMATION**

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

PARTICIPATION IN CHAT ROOMS AND NEWSGROUPS	No participation in any chat room or newsgroup accessed on the Internet is permissible for students or employees
NETWORK ETIQUETTE	<p>System users are expected to observe the following network etiquette:</p> <ol style="list-style-type: none">1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.3. Pretending to be someone else when sending/receiving messages is considered inappropriate.4. Transmitting obscene messages or pictures is prohibited.5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.
TERMINATION/ REVOCATION OF SYSTEM USER ACCOUNT	Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.
DISCLAIMER	<p>The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.</p> <p>Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.</p> <p>The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.</p>