



**Vallivue School District 139
Information Technology
Acceptable Use and Internet Safety
Administrative Directive**

*(Developed from District Board Policy 603.12)
Approved by Board of Trustees 3/12/02*

VALLIVUE SCHOOL DISTRICT 139

INFORMATION TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY ADMINISTRATIVE DIRECTIVE

Vallivue's Information Technology System provides an electronic highway connecting millions of computers around the world as well as each of the computer workstations and peripherals within the district.

Internet access and Internet e-mail are a part of the system. These systems are filtered and monitored and are modified for public school educational use to assure the safety of students and to limit use to educational purpose related to the mission of the district. They may not always provide the same utility and resources as private or business systems.

This district and its administrators do not have complete control of the content of all information that may be accessed on or by the system. Some sources may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal materials. The Vallivue School District does not condone the presence or use of such materials and does not knowingly permit the presence or use of such materials in the school environment.

Parents of students should be aware that such inappropriate materials exist and that users may encounter information on the Internet and other information services that may be perceived as controversial or potentially harmful. Vallivue has installed modern and sophisticated blocking software intended to filter out inappropriate material, but it is impossible to completely control all content. While the district cannot control the Internet and other network sources of information, we will strive to provide students and staff with the understanding and skills needed to use Information Technology Systems in an appropriate manner.

I. PRIVILEGES AND RESPONSIBILITIES

- All users of the district's systems are expected to have read all of the then current, *Vallivue School District 139 Information Technology Acceptable Use and Internet Safety Policy and Administrative Directive*. By using any part of the system, each user signifies understanding and acceptance of all of its terms and conditions. ***(This or a similar notice will be distributed among staff and will be posted conspicuously near usual points of use.)***
- Below the fifth grade, district acceptable use policies and procedures of the appropriate level will be included in the technology education objectives for each grade. At these grade levels district staff will be directly responsible for all student use and compliance with the ***Vallivue School District 139 Information Technology Acceptable Use and Internet Safety Policy and Administrative Directive***. Elementary School Principals will develop a common statement of rules and/or permissions appropriate to technology use in the elementary schools and submit it to the district administration as an addendum to this document.
- No student above the fourth grade level may use the system without certifying in writing that they have read, or have had read to them and/or explained to them, and do understand the current ***Vallivue School District 139 Information Technology Acceptable Use and Internet Safety Policy and Administrative Directive***. Each student must also have the written permission of a parent or guardian who also certifies that they have read, or have had read to them and/or explained to them, and do understand the current ***Vallivue School District 139 Information Technology Acceptable Use and Internet Safety Policy and Administrative Directive***.
- ***Use of the Information Technology Systems must be for educational purposes only and be consistent with the District's mission.***
- The district will monitor and review all access and activities. Access may be denied, revoked, or suspended to specific users at anytime because of activities that violate this Policy or community standards.

II. SECURITY

The administrators and support personnel of the Information Technology System are employees of the district and are assigned the responsibility of monitoring activity on the system. All users of the Information Technology System will be given a unique user account and password. The account and password are used to control and monitor access and use and are of primary importance in the security of the system.

- Your account and password must remain confidential and cannot be shared with anyone else.
- If you suspect that either the account or the password has become known by someone else, you must report that fact immediately to the system administrator.
- You must not allow any other person to use any workstation that has been logged in with your account and password.
- You must not use any workstation that has been logged in with someone else's account and password.
- Users may not leave a workstation unattended while it is open to their account.
- If a user feels that he/she can identify a security problem on the Information Technology System, the user shall notify a systems administrator and shall not demonstrate the problem to others.
- Users shall be required to change passwords regularly and shall immediately notify a systems administrator if their password is no longer secure, or if they have reason to believe that someone has obtained unauthorized access to their account.
- No user may attempt to gain unauthorized access to any computer network service or facility, nor attempt to go beyond any authorized access. This includes accessing, or attempting to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of Vallivue School District or any other entity's system, whether or not the intrusion results in verifiable harm. These actions are illegal, even if only for the purposes of "browsing".
- Attempting to infiltrate a computing system and/or damage software components is prohibited.
- From time to time Vallivue systems administrators will issue warnings, instructions and/or actions to be taken in relation to a virus or other threat or adjustment to the system. All system users have a responsibility to respond immediately and completely to such communications.

III. ACCEPTABLE USE

- Users may not use the System to transmit any material (by email, uploading, posting, or otherwise) that, intentionally or unintentionally, violates any applicable local, state, national, or international law, or any rules or regulations promulgated thereunder.
- The System may not be used for private or commercial purposes. Using the system to make offers to sell or buy products, items, or services, or to advance any type of activity such as "pyramid schemes," "ponzi schemes," or "chain letters" is prohibited.
- The Information Technology System may not be used in a way that would impair the use of the system by others.

III. ACCEPTABLE USE (continued)

- Users may not use the System to transmit any material (by email, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property or that harasses another.
- Users may not swear, use vulgarities, or any other inappropriate language.
- The privacy of others must be respected by all users.
- No user may upload, download, or install software into any district system except under the direction of a technology administrator.
- No privately owned computers, printers or other devices may be attached to the district system except by support personnel when they have been authorized to do so by the Information Systems Administrator.

IV. SAFETY

- It is the responsibility of all employees to observe student Internet use and to promptly report any activity that could jeopardize the personal safety of any student. **This is the primary system safety mechanism.** Monitoring, auditing and filtering alone are not sufficient to guarantee student safety.
- No student of any age may use the district Information Technology System except under the direction and supervision of a staff member.
- Student Internet users may not reveal any personal information such as home address, telephone number or name, to anyone on the Internet.
- Student users will not participate in any "chat" activity.
- Student users will not make arrangements to meet with anyone they have "met" on the Internet.
- Students will not be issued personal e-mail accounts and are prohibited from using Instant Messaging, Napster-like services, Web-based e-mail and similar utilities and services that represent an exposure to unfiltered or uncontrolled information or communication sources.
- Student users will promptly disclose to their teacher or other school employee any message or material they receive or observe that is inappropriate or makes them feel uncomfortable.

V. COPYRIGHT

- It is the intent of the Vallivue School District that this school district adheres to the provisions of the United States Copyright Act (Title 17 of the United States Code) and congressional guidelines. This policy specifically includes respecting all computer software copyrights and adhering to the terms of all software licenses to which the district is a party. The district does not condone the illegal use or reproduction of copyrighted materials in any form. Unauthorized duplication of software may subject users and/or the district to both civil and criminal penalties under the United States Copyright Act. The district does not permit any employee to use software in any manner inconsistent with the applicable license agreement. Employees who willfully disregard this policy, do so at their own risk and assume all liability.

V. COPYRIGHT (continued)

- Users may not use, transmit or copy any material (by email, uploading/downloading, posting, or otherwise) that infringes any copyright, trademark, patent, trade secret, or other proprietary rights of any third party. This includes, but is not limited to, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources, and the unauthorized transmittal of copyrighted software. A user may download or redistribute such material only with the express written permission of the owner or authorized person or as provided by the fair use exception to the copyright laws.
- No computer software, including "Shareware" or "Freeware", shall be placed on any system connected to Vallivue's Information Technology System by any user. All software installed on district systems must be installed by authorized support personnel, or under their direction.
- Software management duties will be assigned to a staff member who will supervise software use and licensing and maintain records and copies of regulations, policies, information sources and guidelines related to copyright issues.

VI. ELECTRONIC MAIL

- E-mail is not a secure nor private system and any transmitted material may at times be viewed by others. There is no guarantee of confidentiality. Users should carefully evaluate the content of all intended e-mail and not use the system to transmit confidential, private or sensitive information. There are other ways to transmit necessary confidential or private information within the district using the system. An appropriate procedure may be set up by a systems administrator upon request.
- Systems administrators will not intentionally inspect the contents of E-mail sent by one user to an identified addressee. Nor will they disclose e-mail contents unless required to do so by law or by policies of this district, or to investigate complaints regarding E-mail which are alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any E-mail transmitted on this district's Information Technology System.
- Users may not use the e-mail services to transmit any commercial email or bulk email.
- E-mail service is provided to support education and the mission of the school district. Forwarding received mail or attachments to others is prohibited unless it contributes to the education of students and the mission of the district.
- Users who subscribe to any list serve must report the subscription to the systems administrator within twenty four hours of subscribing. When a list is unsubscribed, notice must also be provided to the systems administrator. The systems administrator will maintain a record of all current subscriptions and will coordinate with district administrators to assure that all lists are unsubscribed before a user leaves the district or is absent for an extended period of time.
- Users are expected to remove old messages in a timely fashion. The system administrators may remove such messages if not tended regularly by the users.
- A canceled Information Technology System account will not retain its E-mail access.

VII. WEB PAGES

- All web pages are to be educational in nature and directly related to the mission of the district.
- Web pages may not express personal views, promote commercial ventures, nor contain graphics or writing, which may be distasteful to others.
- Web pages may not display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material; nor may they encourage the use of controlled substances or any other activity that is contrary to school and community standards.
- Hyperlinking to a personal web site is not permitted.
- The content of all web pages will be subject to review at any time.

VIII. DISK USAGE

- The system administrators will set quotas for disk usage on the network system.
- Users exceeding their quota will be required to delete files to return to compliance. Users may request that their disk quota be increased by submitting a request stating the need for the quota increase. In determining whether to grant the request the designated administrator shall review the space available, and the reason for the request. A user who remains in noncompliance of disk space quotas after (7) days of notification will have the files removed by a system administrator.
- All student home directories will be deleted at the end of each school year. It is the responsibility of the student to transfer any files they wish to keep to other storage devices.
- The system administrator may delete staff home directories that exceed their quota limits or delete home directories of staff members no longer employed by the district.
- Users are expected to practice good file management by removing files and directories that are no longer needed.

IX. VANDALISM

- Users may not attempt to harm or destroy data or programs of another user, the district Information Technology System, or other Information Technology Systems. This includes, but is not limited to, the uploading or creation of computer viruses. Any attempt to damage or modify any part of the computer system or hardware, specifically including mice, keyboards, speakers, disk drives, monitors, and printers is prohibited.

X. DISCIPLINE PROCEDURE

- As much as possible, violations of this acceptable use policy will be monitored and prosecuted at the **attempt** level. This means that attempting to violate this policy is in fact a violation of the policy itself and will be considered as much an infraction as an actual violation.
- Users of the district Information Technology System who are found to be in violation of *the Vallivue School District 139 Acceptable Use and Internet Safety Policy* will be referred to the Vallivue School District administration and/or local and state law enforcement for follow up and possible disciplinary action.

Vallivue Information Technology Acceptable Use/Internet Safety Administrative Directive
Page 6 of 6

X. DISCIPLINE PROCEDURE (continued)

- The system administrator may temporarily suspend a user's access to, and use of, the Information Technology System upon any violation of this policy. Access will remain suspended until the system administrator is directed by the appropriate administrative authority to reinstate the account.

XI. SOURCES

- This *Vallivue School District 139 Acceptable Use and Internet Safety Administrative Directive* is authorized and required by Vallivue School District Policy 603.12, adopted by the Board of Trustees on March 12, 2002.
- The Computer Fraud and Abuse Act, first enacted in 1984 and revised in 1994, makes certain activities related to certain classes of computers and computer systems illegal. These activities may range from knowingly accessing a computer without authorization or exceeding authorized access to the transmission of a harmful component of a program, information, code, or command. [Http://post.wwstout.edu/s/stenberge/computer_fraud_abuse_act.htm](http://post.wwstout.edu/s/stenberge/computer_fraud_abuse_act.htm)
- The Software & Information Industry Association is an industry "watchdog" that represents more than 1200 software related companies. This association tracks down and prosecutes software piracy cases at every level and has been very successful. They also publish a great volume of explanatory material as well as suggested practices. [Http://siii.net](http://siii.net)
- The Library of Congress and the U.S. Copyright Office publish copyright laws, explanations, case law and related pending legislation. [Http://loc.gov/copyright](http://loc.gov/copyright)
- Larry Magid, syndicated columnist for the Los Angeles Times and a CBS News Technology Analyst maintains a website centered on the safe use of the Internet by minors. [Http://safekids.com](http://safekids.com)
- The district technology support office at Vallivue High School will maintain copies of documents from these sites as well as other related materials.

Table of Contents

I.	PRIVILEGES AND RESPONSIBILITIES	1
II.	SECURITY	2
III.	ACCEPTABLE USE	2
IV.	SAFETY	3
V.	COPYRIGHT	3
VI.	ELECTRONIC MAIL	4
VII.	PERSONAL WEB PAGES	5
VIII.	DISK USAGE	5
IX.	VANDALISM	5
X.	DISCIPLINE PROCEDURE	5
XI.	SOURCES	6