

## Instruction

### Access to Electronic Networks

Electronic networks, including the Internet, are a part of the Valley View School District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s).

Valley View School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

### Curriculum

The use of Valley View School District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

### Acceptable Use

All use of Valley View School District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic Network Access* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

### Internet Safety

Each Valley View School District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee, or (4) harmful to computers and equipment. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict access by minors to inappropriate matter as well as restricting access to harmful materials,
3. Ensure the privacy, safety, and security of minors and staff when using electronic communications including electronic mail, chat rooms, and other forms of direct electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities of minors online,
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses, and

6. Restrict minors' access to materials harmful to them.

Authorization for Electronic Network Access

Each staff member must sign Valley View School District's *Authorization for Electronic Network Access* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use.

All users of the District's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

The failure of any student or staff member to follow the terms of the *Authorization for Electronic Network Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

- LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.  
Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).  
Enhancing Education Through Technology Act, 20 U.S.C §6751 et seq.  
720 ILCS 135/0.01.
- CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:210 (Instructional Materials), 6:230 (Library Resource Center), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Restrictions on Publications and Written or Electronic Material)
- ADMIN PROC.: 6:235-AP (Administrative Procedure - Acceptable Use of Electronic Networks),  
6:235-E2 (Exhibit - Authorization for Electronic Network Access)
- ADOPTED: August 25, 1997
- AMENDED: April 23, 2001
- AMENDED: August 27, 2001
- AMENDED: September 24, 2007
- AMENDED: January 28, 2008