

Acceptable Computer Use - Regulation 3135.00 R

The Danville School Board provides a computer system, including the internet, to promote educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes, but is not limited to, hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape or flash drives, servers, mainframe and personal computers, tablets, cellular phones, smart telephones, the internet and other internal or external networks.

All use of the Division's computer system must be (1) in support of education and/or research, or (2) for legitimate school business. Use of the computer system is a privilege, not a right. Any communication or material generated using the computer system, including electronic mail, instant or text messages, tweets, or other files deleted from a user's account, may be monitored, read, and/or archived by school officials.

The Division Superintendent shall establish administrative procedures, for the School Board's approval, containing the appropriate uses, ethics and protocol for the computer system.

The procedures shall include:

1. a prohibition against use by Division employees and students of the division's computer equipment and communications services for sending, receiving, viewing or downloading illegal material via the internet;
2. provisions, including the selection and operation of a technology protection measure for the division's computers having Internet access to filter or block Internet access through such computers, that seek to prevent access to:
 - a. child pornography as set out in V Code § 18.2-374.1:1 or as defined in 18 U.S.C. § 2256;
 - b. obscenity as defined by Va. Code § 18.2-372 or 18 U.S.C. § 1460; and
 - c. material that the school division deems to be harmful to juveniles as defined in Va. Code § 18.2-390, material that is harmful to minors as defined in 47 U.S.C. § 254(h)(7)(G), and material that is otherwise inappropriate for minors;
3. provisions establishing that the technology protection measure is enforced during any use of the Division's computers;
4. provisions establishing that all usage of the computer system may be monitored;
5. provisions designed to educate students and employees about appropriate online behavior, including interacting with students and other individuals on social networking websites, blogs, in chat rooms, and cyberbullying awareness and response;
6. provisions designed to prevent unauthorized online access by minors, including "hacking" and other unlawful online activities;
7. provisions prohibiting the unauthorized disclosure, use, and dissemination of photographs and/or personal information of or regarding minors; and
8. a component of internet safety for students that is integrated in the Division's instructional program.

Use of the School Division's computer system shall be consistent with the educational or instructional mission or administrative function of the Division as well as the varied instructional needs, learning styles, abilities and developmental levels of students.

The Division's computer system is not a public forum.

The failure of any student, teacher or administrator to follow the terms of this policy or accompanying regulation may result in loss of computer system privileges, disciplinary action, and/or appropriate legal action.

The School Board is not responsible for any information that may be lost, damaged or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

The School Board will review, amend if necessary, and approve this policy every two years.

All use of the Danville School Division's computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. The term computer system includes, but is not limited to, hardware, software, data, communication lines and devices, terminals, printers, CD-ROM devices, tape or flash drives, servers, mainframe and personal computers, tablets, cellular phones, smart phones, the internet and any other internal or external network.

Computer System Use-Terms and Conditions:

1. **Acceptable Use:** Access to the Division's computer system shall be (1) for the purposes of education or research and be consistent with the educational objectives of the Division or (2) for legitimate school business.
2. **Privilege:** The use of the Division's computer system is a privilege, not a right.

3. Unacceptable Use: Each user is responsible for his or her actions on the computer system. Prohibited conduct includes but is not limited to:
 - using the network for any illegal or unauthorized activity, including violation of copyright or contracts, or transmitting any material in violation of any federal, state, or local law.
 - sending, receiving, viewing or downloading illegal material via the computer system.
 - unauthorized downloading of software.
 - using the computer system for private financial or commercial purposes.
 - wastefully using resources, such as file space.
 - gaining unauthorized access to resources or entities.
 - posting material created by another without his or her consent.
 - submitting, posting, publishing, or displaying any obscene, profane, threatening, illegal, or other inappropriate material.
 - using the computer system while access privileges are suspended or revoked.
 - vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.
 - intimidating, harassing, bullying, or coercing others.
 - threatening illegal or immoral acts.

4. Network Etiquette: Each user is expected to abide by generally accepted rules of etiquette, including the following:
 - be polite.
 - users shall not forge, intercept or interfere with electronic mail messages.
 - use appropriate language. The use of obscene, lewd, profane, lascivious, threatening or disrespectful language is prohibited.
 - users shall not post personal information other than directory information as defined in Policy JO Student Records about themselves or others.
 - users shall respect the computer system's resource limits.
 - users shall not post chain letters or download large files.
 - users shall not use the computer system to disrupt others.
 - users shall not modify or delete data owned by others.

5. Liability: The School Board makes no warranties for the computer system it provides. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The School Division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs, or damages incurred by the School Board relating to or arising out of any violation of these procedures.

6. Security: Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately. All users shall keep their passwords confidential and shall follow computer virus protection procedures.

7. Vandalism: Intentional destruction of or interference with any part of the computer system through creating or downloading computer viruses or by any other means is prohibited.

8. Charges: The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone, data, or long-distance charges.

9. Electronic Mail: The School Division's electronic mail system is owned and controlled by the School Division. The School Division may provide electronic mail to aid students and staff in fulfilling their duties and as an education tool. Electronic mail is not private. Students' electronic mail will be monitored. The electronic mail of staff may be monitored and accessed by the School Division. All electronic mail may be archived. Unauthorized access to an electronic mail account by any student or employee is prohibited. Users may be held responsible and personally liable for the content of any electronic message they create or that is created under their account or password. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file.

10. Enforcement: Software will be installed on the division's computers having Internet access to filter or block internet access through such computers to child pornography and obscenity. The online activities of users may also be monitored manually. Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by School Board policy, or legal action.