7.6 ACCEPTABLE COMPUTER USE AND INTERNET SAFETY

It is the policy of Davidson County Schools to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

ACCESS TO INAPPROPRIATE MATERIAL

To the extent practical, Internet filters shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, Internet filters may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

INAPPROPRIATE NETWORK USAGE

To the extent practical, steps shall be taken to promote the safety and security of users of the Davidson County Schools online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

EDUCATION, SUPERVISION AND MONITORING

It shall be the responsibility of all members of the Davidson County Schools staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures, including the Internet filter, shall be the responsibility of the IT Director or designated representatives.

School faculty and staff will provide age appropriate training for students who use the Davidson County Schools Internet facilities. The training provided will be designed to promote the district's commitment to:

a. The standards and acceptable use of Internet services as set forth in the Davidson County Schools Acceptable Computer Use and Internet Safety Policy;
b. Student safety with regard to:
   i. safety on the Internet;
   ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
   iii. cyber bullying awareness and response.

c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

The following actions are specifically not permitted on school system equipment on or off school premises:

1. Accessing, producing, posting, sending, or displaying material that is deemed offensive in nature is prohibited. This includes obscene, discriminating, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or suggestive language or images. Students and teachers may not bypass the district's filtering system to gain access to restricted sites. This includes running software that accesses proxy servers that allow the filter to be bypassed.
2. Engaging in any illegal, inappropriate or offensive activities or accessing material advocating illegal acts or violence is not allowed. This includes material related to pornography, hate literature, illegal gambling, illegal weapons, terrorist activities, or other illegal activities or activities or material that ridicules others on the basis of race, creed, religion, gender, disability, national origin, or sexual orientation.
3. Using the Internet/email system to harass, insult, or attack others will not be permitted.
4. Tampering with computers, computer systems, software, or computer networks is prohibited. Only district or school level media, technology personnel, or an individual designated by the Superintendent, should access computer network settings to include passwords, data, and IP addresses. Intentional propagation of viruses is prohibited.
5. Plagiarizing or infringing copyrights of works found on the Internet is illegal.
6. Intentionally wasting limited resources including disk space and printing supplies is not allowed.
7. Using computers or the Internet/email system for commercial purposes or in support of "for profit" activities or other outside employment or business activity is prohibited.
8. Using the system for political lobbying is prohibited.
9. Posting personal or private information about oneself or other people on the Internet, such as name, address, and telephone number is not allowed.
10. Attempting to gain unauthorized access to the school file servers and restricted network areas is prohibited.
11. Downloading and installing software applications, shareware, and freeware without prior approval from Media and Technology staff is not permitted. Examples could include but are not limited to screen savers, multimedia applications, Yahoo toolbar, and Web Shots.
12. Unauthorized use of real-time Internet services such as chat rooms, instant messaging, social networking, and blogging for non-instructional purposes is prohibited. Prior approval can be obtained from the district Media and Instructional Technology staff.
13. Down-streaming music and/or video for non-instructional purposes is prohibited during school hours by all users. These activities can degrade the performance of the overall functionality of the wide area network.
14. Using computers and/or Internet sites for non-instructional games is prohibited.
15. Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings regardless of subject matter is prohibited.

16. Using outside email systems not approved for curriculum purposes is prohibited.
17. The installation of software on a school computer by anyone other than school or district technology or media personnel is prohibited.
18. Access to the internet for non-instructional purposes during class time is prohibited.
19. Use of personal technology equipment, to include laptops, wireless devices, and workstations within the school system is expressly prohibited without prior written consent of the Davidson County Schools Technology Department

Use of the Internet is a privilege, not a right. Inappropriate use of the Internet may result in disciplinary or legal action and Davidson County Schools reserves the right to monitor any student or employee's use of the Internet.

Legal Reference: PL 106-554

Adopted/Revised: January 2, 1996; September 2, 1997; March 1, 1999; April 2, 2001; June 24, 2002; March 7, 2005; October 3, 2005; September 6, 2006; December 03, 2008; April 02, 2012; June 28, 2012; May 5, 2014