COMPUTER/ONLINE SERVICES
(Acceptable Use and Internet Safety)

Technology can greatly enhance the instructional program, as well as the efficiency of the District. The Board recognizes that careful planning is essential to ensure the successful, equitable and cost-effective implementation of technology-based materials, equipment, systems and networks.

Computers and use of the District network or online services support learning and enhance instruction, as well as assist in administration. For purposes of this policy computers include District-owned desktop computers, laptops, tablets and other mobile computing devices.

All computers are to be used in a responsible, efficient, ethical and legal manner. Failure to adhere to this policy and the guidelines below will result in the revocation of the user's access privilege. Unacceptable uses of the computer/network include but are not limited to:

1. violating the conditions of State and Federal law dealing with students' and employees' rights to privacy, including unauthorized disclosure, use and dissemination of personal information;

2. using profanity, obscenity or other language that may be offensive to another user or intended to harass, intimidate or bully other users;

3. accessing personal social networking websites for noneducational purposes;

4. reposting (forwarding) personal communication without the author's prior consent;

5. copying commercial software and/or other material in violation of copyright law;

6. using the network for financial gain, for commercial activity or for any illegal activity;

7. "hacking" or gaining unauthorized access to other computers or computer systems, or attempting to gain such unauthorized access;

8. accessing and/or viewing inappropriate material and

9. downloading of freeware or shareware programs.

The Superintendent/designee shall develop a plan to address the short- and long-term technology needs and provide for compatibility of resources among school sites, offices and other operations. As a basis for this plan, he/she shall examine and compare the costs and benefits of various resources and shall identify the blend of technologies and level of service necessary to support the instructional program.

Because access to online services provides connections to other computer systems located all over the world, users (and parents of users who are under 18 years old) must understand that neither the school nor the District can control the content of the information available on these systems. Some of the information available is controversial and sometimes offensive.

The Board does not condone the use of such materials. Employees, students and parents of students must be aware that the privileges to access online services are withdrawn from users who do not respect the rights of others or who do not follow the rules and regulations established. A user's agreement is signed to indicate the user's acknowledgment of the risks and regulations for computer/online services use. The District has implemented technology-blocking measures that protect against access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, harmful to minors. The District has also purchased monitoring devices that maintain a running log of internet activity, recording which sites a particular user has visited.

"Harmful to minors" is defined as any picture, image, graphic image file or other visual depiction that:

1. taken as a whole and with respect to minors appeals to a prurient interest in nudity, sex or excretion;

2. depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts or a lewd exhibition of genitals and

3. taken as a whole, lacks serious literary, artistic, political or scientific value as to minors.

The District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The Superintendent/designee will develop a program to educate students on these issues.

Annually, a student who wishes to have computer network and internet access during the school year must read the acceptable use and internet safety policy and submit a properly signed agreement form. Students and staff are asked to sign a new agreement each year after reviewing the policies and regulations of the District. **The District reserves the right to amend policies and regulations as necessary throughout the school year. Users are notified of the updated policies and regulations and must comply with the updated requirements.** These policies and regulations also apply to use of District-owned devices, or accessing of District intranet **and software programs** off District property. **All users using platforms established for e-learning regardless of whether the student or employee is using a personal or District provided device must be used in accordance with the standards for conduct outlined in this policy and the accompanying regulation. Users in violation of this policy or the accompanying regulation may be subject to discipline.**

[Adoption date:]

LEGAL REFS.: U.S. Const. Art. I, Section 8
Family Educational Rights and Privacy Act; 20 USC 1232g et seq.
Children's Internet Protection Act; 47 USC 254 (h)(5)(b)(iii); (P.L. 106-554, HR 4577, 2000, 114 Stat 2763)
ORC 3313.20
        3319.321

CROSS REFS.: AC, Nondiscrimination
ACA, Nondiscrimination on the Basis of Sex
ACAA, Sexual Harassment
EDEB, Bring Your Own Technology (BYOT) Program
GBCB, Staff Conduct
GBH, Staff-Student Relations (Also JM)
IB, Academic Freedom
IIA, Instructional Materials
IIBH, District Websites
JFC, Student Conduct (Zero Tolerance)
JFCF, Hazing and Bullying (Harassment, Intimidation and Dating Violence)
Staff Handbooks
Student Handbooks

NOTE: *The Children's Internet Protection Act (CIPA) requires districts that receive federal funds to purchase computers, direct access to the internet under the Elementary and Secondary Education Act or receive federal universal E-Rate service discounts and internet connections services under the Communications Act to adopt, implement and maintain computer use policies that address these issues:*

1. *access by minors to material deemed as harmful to minors on the internet and World Wide Web;*

2. *access by both adults and minors to visual depictions that are obscene, child pornography on the internet and World Wide Web;*

3. *safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;*

4. *unauthorized access, including "hacking" and other unlawful activities by minors online;*

5. *unauthorized disclosure, use and dissemination of personal information regarding minors;*

6. *measures designed to restrict access to materials deemed "harmful to minors" and*

7. *educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.*

The district must create a plan for educating students concerning appropriate online behavior; this plan is separate from the policy manual. The FCC has provided resources including OnGuardOnline.gov to aid districts in developing local plans.

In addition, the popularity of social networking websites has made it necessary for administrators to address the access of these sites on district property. Specific language restricting use, along with the disciplinary penalties imposed on offenders, should be placed in staff and student handbooks.

It is important to note that the FCC recognizes that while some individual Facebook and MySpace pages could potentially contain material harmful to minors, social networking websites are not per se harmful to minors, and therefore do not automatically have to be blocked. This decision is left up to the district's discretion.

Additional policy language addressing social networking is found in GBH (Also JM), Staff-Student Relations and IIBH, District Websites.

Additionally, the board shall make a local determination as to what is classified "inappropriate for minors" in line with the current definition.

In report 11-125, FCC adopted the following definition of minor: "any individual who has not attained the age of 17 years." All E-Rate program participants must use this definition of minor for the purpose of this topic.

The district internet safety policy must be made available to the FCC upon request.

Districts who are implementing a Bring Your Own Technology program should review and adopt EDEB, Bring Your Own Technology Program.

THIS IS A REQUIRED POLICY