

The use of electronic information resources offers a unique opportunity to enhance instructional methods, appeal to different learning styles, and meet the educational goals of the board. Through the use of this technology, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

The use of the electronic information resources should be integrated into the educational program when teaching and in meeting the educational goals of the board. The Instructional Team should provide suggestions for using technology along with the curriculum guides as provided in board policy 3115, Curriculum and Instructional Guides. Teachers are encouraged to further incorporate the use of the technology into their lesson plans.

The Director of Technology and Media shall ensure that school district computers with Internet/network access comply with federal requirements regarding filtering software and network safety policies. The Director of Technology and Media shall develop any regulations necessary to meet such requirements and will submit any certifications necessary to meet the requirements of the Children's Internet Protection Act (CIPA).

#### REQUIREMENTS FOR USE OF THE DISTRICT-OWNED ELECTRONIC RESOURCES

The use of the district-owned information resources is a privilege, not a right. District-owned electronic resources include computer equipment, including any desktop or laptop computers or other hardware, that is owned or leased by the school system; cell phones and other portable communication devices provided by the school district; e-mail accounts; the Orange County Schools computer network; and any computer software licensed to the Orange County School System.

Users of Orange County Schools' electronic resources are expected to respect the school system's property and be responsible in using the equipment. Users are to follow any school system instructions regarding maintenance or care of the equipment. Users may be held responsible for any damage caused by intentional or negligent acts in caring for Orange County Schools electronic resources under their control.

All users of district-owned information resources, both staff and students, must comply with the following requirements.

- The OCS network and internet access are provided and can only be used for school-related purposes. OCS electronic resources, the Internet, and use of e-mail are not inherently secure or private. Students and employees shall have no expectation of privacy while using OCS electronic resources. The Orange County School System reserves the right to search data or e-mail stored on all school-owned or leased computers or other electronic resources at any time for any reason. The Orange County School System reserves the right to monitor the use of OCS electronic resources and to take appropriate disciplinary action based on use that is in violation of this policy. The Orange County School System reserves the right to disclose any electronic message or data to law enforcement officials, and under some circumstances, may be required to disclose information to law enforcement officials or other third parties, for example, in response to a subpoena or court order.
- Students must meet all standards of expected student behavior and comply with all board policies and school standards and rules while using electronic resources.
- Employees must comply with all relevant board policies when using the district-owned information resources.

- No user of the district-owned information resources, including a person sending or receiving electronic communications, may engage in creating, intentionally accessing or transmitting images, documents or other material that is obscene, defamatory, pornographic, harassing or considered to be harmful to minors.
- All applicable laws and board policies apply, including those relating to copyrights/trademarks, confidential information and public records. Any use that violates state or federal laws is strictly prohibited.
- When using email, chat rooms or other forms of electronic communication, students must not reveal personally identifiable, private or confidential information, such as home address or telephone number, of themselves or fellow students. In addition, school personnel shall not disclose on the internet/network or on school district web sites/pages any personally identifiable information concerning students (including name, address or pictures) without the permission of a parent/guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or board policy 4700, Student Records.
- Users of the school computer system or internet/network access are prohibited from engaging in unauthorized or unlawful activities such as “hacking” or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers or computer systems.
- If a user can identify a security problem on the network or the school computer system, he/she must immediately notify a system administrator. Users shall not demonstrate the problem to other users. Any user identified as a security risk shall be denied access.
- Users (other than technology staff in performance of their duties) are prohibited from using another individual’s computer account.
- Use of the district-owned information resources for commercial gain or profit is not allowed.
- Views may be expressed as representing the view of the school district or part of the school district only with prior approval by the superintendent or his or her designee.

### **RESTRICTED MATERIAL**

Before a student may access the internet or OCS network at school for any purpose, the parent/guardian must be made aware of the possibility that the student could obtain access to inappropriate material. The parent/guardian and student must sign a consent form acknowledging that the student user is responsible for appropriate use of the technology and consenting to the school district monitoring the student’s e-mail communication and use of the network.

The board is aware that there is information on the internet that is not related to the educational program. The board also is aware that there is information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents/guardians would find objectionable. The school district will take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language which does not serve a legitimate pedagogical purpose. The school district will install or will ensure that its network service provider installs a technology protection measure that blocks or filters network access to audio or visual depictions that are obscene, that are considered child pornography or that are harmful to minors. Although it is the intent of the Orange County Schools that school system electronic information resources be used only to pursue educational goals and objectives, filters may not block all offensive material and parents are warned that students may find ways to access inappropriate materials. School officials

may disable such filters for an adult who uses a school-owned computer for bona fide research or other lawful educational purpose. The school district shall not seek to limit access to the district-owned information resources for the purpose of restricting access to political ideas or social perspectives if the action is not rated simply by a school district official's disapproval of the ideas involved. However, the user is ultimately responsible for his or her activity on the network/internet.

## SOCIAL NETWORKING WEBSITES

### 1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school district computers during non-school hours, when the students' on line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see Student Code of Conduct Policy in the 4000 series).

### 2. Employees and school organizations

Any employee or school organization (e.g. sports affiliates, art affiliates) must have permission from the principal/supervisor before creating or posting on a social networking site. If this is a Facebook page, the principal/supervisor will then notify the Director of Technology and a page will be created under the district Facebook page to allow monitoring and administration of the page if the administrator (creator) were to leave the district.

All employees must use the OCS network or OCS sponsored websites if possible when communicating with students/parents about any school related matters. Thus, employees may not use personal websites or on-line networking profiles to post information in an attempt to communicate with students/parents about school-related matters.

Employees must abide by Policy 3224, Employee Use of Social Networking Sites, when using social networking sites on or off campus.

Legal Reference: U.S. Const. Amend. I; 17 U.S.C. 100 et seq.; Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Children's Internet Protection Act, 47 U.S.C. §254(h)(5); Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; G.S. 115C-391, -325(e)

Cross Reference: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Citizenship and Character Education (policy 3530), Copyright Compliance (policy 3230/7330), Student Code of Conduct (policy 4300), Integrity and Civility (policy 4310), Public Records (policy 5070), Use of the Computers (policy 6523), Network Security (policy 6402), Staff Responsibilities (policy 7300)