ACCEPTABLE USE AND INTERNET SAFETY FOR INFORMATIONAL AND EDUCATIONAL TECHNOLOGY

The Dayton Public School District realizes that 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.

The use of computers and other District network or online devices/services support learning and enhance instruction, as well as assist in administration. Electronic networks allow people to interact with many computers and other resources; the Internet allows people to interact with hundreds of thousands of networks and individuals around the world.

Information and Communication Technology (ICT) and Social Media Usage

ICT and social media are recognized technologies that enable the District and students to share information in a timely, relevant manner across numerous platforms. As mediums continue to evolve, the District recognizes the importance of finding new ways to reach families, students, the community and other stakeholders, while remaining mindful of its obligation to uphold regulations regarding student privacy, Internet safety and Board policies.

Social media is to be used within the district as another tool for effective two-way communication. Any site representing the District as a whole will be created and maintained by the Public Information Office or other Superintendent designee; no other entity shall purport to officially represent the District in this capacity.

Social media shall be used:

1) To promote the District in a positive manner;

2) To share District news and information in a timely and relevant fashion;

3) To encourage two-way communication between the District and the public; and

4) In ways that are not in violation of policies regarding student safety (see also JM).

Socal Media Interactions

To maintain a more formal staff-student relationship, district employees shall not “friend” current students on social networking sites such as Facebook and MySpace (except when that employee is a relative or legal guardian of the student). In addition, district employees will not “instant message” or text message current students, and will not respond to student-initiated attempts at conversation through non-district-approved media, whether personal or professional accounts.

Assume that nothing posted online, in any capacity, is private. When putting something online, use the "Front Page Test" - would this post/picture/information be embarrassing, slanderous or threatening if it ended up on the front page of tomorrow's newspaper?

Social Media Privacy

Use of Facebook, Twitter or other social media sites: It is recommended that students and staff keep privacy settings to "Only Friends," or to personally approve friends and followers.

DPS employees are not permitted to post pictures of students with personally identifying information. Students are not to be "tagged" in photos.

Other district guidelines and policies regarding disclosure of student record information must be adhered to when using a personal account, including posting of student photographs, names of students and personally identifiable information.

Social Media Usage

Staff and students should use only approved social media sites. Approved sites are authorzed by their educational content and have been vetted through the district's Software/Hardware Review Process. Staff who seek to use these and other restricted sites as part of the educational process should contact the Office of Information Technology for assistance.

All technologies 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 which may be offensive to another user or intended to harass, intimidate or bully other users;

3. accessing personal social networking websites for non-educational 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;

9. unauthorized downloading of freeware or shareware programs and all copyrighted material, including music and videos;

10. sending or forwarding chain letters or "spam" to a large group of users;

11. storage of "personal files" including pictures, jokes, videos, games and other recreational software and

12. use of personal e-mail accounts of any e-mail account for personal communication.

13. when using social media:
    a) do not create content (posts, message responses, Tweets ©, photo manipulations, etc.) that portray the district or an individual in an obscene, defamatory or libelous way.

    b) be transparent and honest in your online interactions. Do not post anonymously. If you are identified as a district employee, be sure to mention your views and opinions are your own and do not represent the district as a whole.

The Superintendent, or his/her 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 to prevent students from accessing inappropriate material or materials considered to be harmful to minors on school computers. The District has also purchased monitoring devices which 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 lewd exhibition of genitals or

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

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.

Search and Seizure

Students and employees should have no expectation of privacy with respect to the use of any district Information Communication Technology. Violations of District regulations, disciplinary code or the law may result in severe penalties, including, but not limited to termination of employees or expulsion of students.

Routine maintenance and monitoring of ICT systems may lead to discovery that the user has or is violating the District Acceptable Use Regulations, the Student Code of Conduct or the law. An individual search is conducted if there is reasonable suspicion that a user has violated the law or the disciplinary code. The nature of the investigation is reasonable and in the context of the nature of the alleged violation.

District employees should be aware that their personal files might be discoverable under state public records laws.

[Adoption date: August 5, 2009]
[Re-adoption date: June 21, 2011]

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; (P.L. 106-554, HR 4577, 2000, 114 Stat 2763)
ORC 1329.54 through 1329.67
3313.20
3319.321

CROSS REFS.: AC, Nondiscrimination/Harassment
ACA, Nondiscrimination on the Basis of Sex
ACAA, Sexual Harassment
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)
Employee Manual
Student Handbooks