INFORMATION AND COMMUNICATION TECHNOLOGY REGULATIONS
(Acceptable Use and Internet Safety)

Purpose

The Information and Communication Technology (ICT) systems of the District are limited to an educational purpose. The purpose of the District's Information and Communication Technology systems is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. Additionally, the ICT systems increases District intra-communication, enhances productivity and assists District employees in upgrading their skills through greater exchange of information with their peers. The ICT systems of the District also assist in the sharing of information with the local community, including parents, social service agencies, government agencies and businesses.

The term "educational purpose" includes use of ICT systems for classroom activities, professional or career development and limited high-quality self-discovery activities. Use of equipment for self-discovery may not in any way violate restrictions established in the Acceptable Use Policy (AUP). Employees will limit their use of ICT systems for self-discovery purposes to no more than three hours per week of non-work time (i.e., lunch, before or after work).

Users may not use the District ICT systems for commercial purposes, defined as offering or providing goods or services for personal use. District acquisition policies are followed for District purchase of goods or services through the District ICT systems.

Users may not use ICT systems for solicitation and/or campaigning. District employees and students may use ICT systems to communicate with their elected representatives and to express their opinion for the purpose of education or educational issues. All use of the District system with regard to political activities must adhere to guidelines established in the Board's policy manual, which includes, but is not limited to, File GBG.

District Responsibilities

The Superintendent or his/her designee is responsible for overseeing the District ICT systems and for working with other regional or state organizations as necessary.

The Office of Information Technology (OIT) serves as the District coordinator for the District ICT systems, establishes a process for setting up individual and class accounts, maintains executed user agreements and sets quotas for disk usage on ICT systems. The OIT Department establishes District virus protection procedures, ensures teachers have opportunities to receive proper training in the use of ICT systems and other procedures deemed necessary by the Board, the Superintendent and/or administrators.

The principals of their respective buildings and/or department heads serve as the building/department level coordinator for the District ICT systems. They approve building-level activities, ensure teachers/staff receive proper training in the requirements of this policy, establish a system to ensure adequate supervision of students using ICT systems and are responsible for enforcing the District Acceptable Use Policies at the building/department level.

Teachers and media center staff instruct students on acceptable use of the network and Board policy.

Technical Services Provided Through District Information and Communication Systems

E-mail: E-mail allows District employees to communicate with people throughout the world and to subscribe to mail lists to engage in group discussion related to educational subjects.

World Wide Web: The Web provides access to a wide range of information in the form of text, graphics, photographs, video and sound from throughout the world. The Web is a valuable research tool for students and employees.

Internet Relay Chat (IRC): IRC (chat) provides the capability of engaging in "real-time" discussions. The District may provide access to IRC only for specifically defined educational classroom activities.

Blocking Software: The District has acquired software designed to prevent students from accessing inappropriate material or materials considered harmful to minors on school computers. However, students, parents and staff must understand that no software is 100% effective.

Wide Area Network (WAN): The District's WAN includes access to business systems (financial, employee and student) for approved staff.

Intranet Services: Intranet services, accessed via DPS InfoNet, allow District staff access to electronic forms and web-based applications.

Extranet Services: Secure remote access to the District's e-mail and Intranet services.

Access to ICT systems
The District's Acceptable Use Policies govern all use of the District ICT systems for staff and students. All users must accept the appropriate Acceptable Use Agreement.

World Wide Web: District employees and students with authorization from their supervisor or parent have access to the Web through the District's networked computers.

Individual E-Mail Accounts for District Employees: District employees, are provided with an individual account and have the ability to forward mail to their personal e-mail if necessary for business purposes.

Guest E-Mail Accounts: No guest accounts are permitted.

Individual E-mail Accounts for Students: E-mail accounts are permitted by the District approved, Children's Internet Protection Act (CIPA) compliant vendor. Students shall not use free Internet or Web mail e-mail providers (including, but not limited to, Hotmail, Gmail, Juno, etc.) to obtain an e-mail address or to send/receive e-mail with an existing address from the District ICT systems.

Parental Notification and Responsibility

The District notifies parents about the District network and the regulations governing its use. Parents must sign an agreement to allow their child(ren) to have Internet access. Parents may request alternative activities for their child(ren) that do not require Internet access.

Parents have the right at any time to investigate the contents of their child(ren)'s electronic files. Parents have the right to request the termination of their child(ren)'s network privileges at any time.

The District's Acceptable Use Policies contain restrictions on accessing inappropriate material. In accordance with CIPA, the District makes every reasonable effort to ensure the safety of students. For this reason, a content filter has been programmed to block unsupervised chat rooms and bulletin boards. Release of such sites containing material that is educationally valuable is addressed on a case-by-case basis.

There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practical or possible for the District to monitor and enforce a wider range of social values in student use of the Internet.

Further, the District recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The District encourages parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District system within the limits established by the District Acceptable Use Regulations.

The District provides students and parents with the Computer and Internet Acceptable Use Guidelines for student safety while using the Internet.

District Limitation of Liability

The District make no warranties of any kind, either express or implied, that the function or the services provided by or through the District system are error-free or without defect. The District is not responsible for any damage users may suffer including, but not limited to, loss of data, interruptions of service or computer viruses. The District is not responsible for the accuracy or quality of the information obtained through or stored on ICT systems. The District is not responsible for financial obligations arising through the unauthorized use of ICT systems.

The District assumes no responsibility or liability for any phone charges including, but not limited to, long distance charges, per minute (unit) surcharges and/or equipment or line costs incurred by users while accessing the District system. Any disputes or problems regarding phone service are strictly between users and his/her local phone company and/or long distance service provider.

Due Process

The District cooperates fully with local, state or federal officials in any investigation concerning or relating to any illegal activities conducted through the District system.

In the event there is an allegation that a student or employee has violated the District Acceptable Use Policy, the student or employee is notified, if permitted by law, of the alleged violation and an opportunity to be heard in the manner set forth in the Student Code of Conduct.

Disciplinary actions are tailored to meet specific concerns related to the violation and to assist the student or employee in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the Student Code of Conduct, the violation is handled in accord with the applicable provision of the Student Code of Conduct.

Employee violations of the District Acceptable Use Regulations are handled in accord with Board policy.

Search and Seizure

Students and employees should have no expectation of privacy with respect to the use of the Internet, Intranet or electronic mail. Violations of District regulations, disciplinary code or the law may result in severe penalties, up to and including 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.

Copyright and Plagiarism

Board policies on copyright govern the use of material accessed through the District system. Copyrighted material must not be placed on any system connected to the District system without the author's permission. Only the owner(s) or person(s) they specifically authorize may upload or download copyrighted material to the District system. It may be permissible to redistribute a copyrighted program non-commercially with the expressed permission of the owner or authorized person. Permission must be specified in the document, on ICT systems or must be obtained directly from the author. Teachers will instruct students to respect copyright and to request permission when appropriate.

Board policies on plagiarism govern use of material accessed through the District system. Teachers will instruct students in appropriate research and citation practices.

Academic Freedom, Selection of Material, Student Rights to Free Speech
Board policies on academic freedom and free speech govern the use of the Internet.

When using the Internet for class activities, teachers select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site. Teachers provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

District Website: The District establishes a website, www.dps.k12.oh.us, and develops web pages that present information about the District. The Office of Public Information is responsible for maintaining the District website and Website Publishing Guidelines. The Webmaster or his/her appointee is responsible for managing and posting to the District website.

District Acceptable Use Guidelines
Users must abide by the following guidelines:

1. Personal Safety:
   Users will not post personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, work address, etc.

   Users will not agree to meet with someone they have met online.
   Student users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable. Employees will report messages to their supervisor.

2. Illegal Activities:
   Users will not attempt to gain unauthorized access to the District system or to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log on through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing."

   Teachers will not give students administrative access to any network that is not isolated from the District system and intended for educational purposes.

   Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

   Users will not use the District system to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.

3. System Security:
   Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person.

   Users will immediately notify the Director, Office of Information and Technology or his/her designee if they have identified a possible security problem. Users will not attempt to discover security problems as these actions may be construed as an illegal attempt to gain access.

   Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures if they download files.

   Users must not attach a modem to a District computer connected to the District system without express written consent from the Superintendent or his/her designee.

4. Inappropriate Language:
   Restrictions against inappropriate language apply to public messages, private messages and material posted on web pages.

   Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.

   Users will not post information that, if acted upon, could cause damage or a danger of disruption.

   Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

   Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, he/she must stop.

   Users will not knowingly or recklessly post fake or defamatory information about a person or organization.

5. Respect for Privacy:
   Users will follow Board policy with regard to confidential material.

   Users will not post private information about another person.

6. Respecting Resource Limits:
   Users will use ICT systems only for education and professional or career development activities (no time limit), and limited, high-quality, self-discovery activities. Employees will limit their use of ICT systems for self-discovery purposes to no more than three hours per week of non-work time (e.g., lunch, before or after work).

Students must obtain approval prior to downloading any files. Any files should be of an educational value. The network is not meant to store personal pictures or backup CDs and DVDs on desktops. Inappropriate and/or personal files may be removed at any time without notice.

Users will not post chain letters or engage in "spamming." Spamming is sending a message that is annoying, unnecessary or has no clear educational purpose to a large number of people.

7. Plagiarism and Copyright Infringement:
   Users will not plagiarize works that they find on the Internet. Plagiarism is taking ideas or writings of others and presenting them as if they were original to the user.

   Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language or artwork that specifies acceptable use of that work, the user should follow the expressed requirements. If the users are unsure whether they can use a work, they should request permission from the copyright owner.

8. Inappropriate Access to Material:
   Users will not view, download or transmit material that is profane or obscene (pornography) that advocates illegal acts or that advocates violence or discrimination toward other people (hate literature) or that could be construed as harassment, bullying or disparagement of others based on their race, color, national origin, ancestry, citizenship status, economic status, sex, sexual orientation, age, disability, religion, political beliefs, military status or any other personal or physical characteristic. For students, a special exception may be made for hate literature if the purpose of such access is to conduct research and both the teacher and the parent approve access. District employees may access the above material only in the context of legitimate research.

   Examples of material considered inappropriate include, but are not limited to, topics dealing with sex, illegal use of drugs, hate speech, online merchandising, gambling, non-educational games, occult, cults, non-educational entertainment, criminal skills, non-educational chat groups, dating and matchmaking.

   If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school. This protects users against an allegation that they have intentionally violated the Acceptable Use Policies.

9. Other Inappropriate Uses:
   Users may not use the District system for commercial purposes, defined as offering or providing goods or services for personal use.

   Users may not use ICT systems for solicitation and/or campaigning.

10. Access to Future Updates of Acceptable Use Regulations:
    Employees may access future updates of the Acceptable Use Regulations through the District's Internet site at www.dps.k12.oh.us or through the District Intranet system.

All other users are notified of changes at the beginning of each school year or may access future updates of the Acceptable Use Regulations through the District's Internet site of www.dps.k12.oh.us or by submitting a written request to the District Webmaster.

(Approval date: August 5, 2009)
[Re-adoption date: June 21, 2011]
[Re-adoption date: October 14, 2014]