Access to Electronic Media

(Acceptable Use Policy)

STUDENT USE

The Board supports the right of students and employees to have reasonable access to various information formats and believes it is incumbent upon users to use this privilege in an appropriate and responsible manner as required by this policy and related procedures, which apply to all parties who use District technology.

SAFETY PROCEDURES AND GUIDELINES

The Superintendent shall develop and implement appropriate procedures to provide guidance for student access to electronic media. Guidelines shall address teacher supervision of student computer use, ethical use of electronic media (including, but not limited to, the Internet, e-mail and other District technological resources), and issues of privacy versus administrative review of electronic files and communications. In addition, guidelines shall prohibit utilization of networks for prohibited or illegal activities, the intentional spreading of embedded messages, or the use of other programs with the potential of damaging or destroying programs or data.

Students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

Internet safety measures, which shall apply to all District-owned devices with Internet access or personal devices that are permitted to access the District's network, shall be implemented that effectively address the following:

1. Controlling access by minors to inappropriate matter on the Internet and World Wide Web;
2. Safety and security of minors when they are using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Preventing unauthorized access, including "hacking' and other unlawful activities by minors online;
4. Unauthorized disclosure, use and dissemination of personal information regarding minors; and
5. Restricting minors' access to materials harmful to them.

A technology protection measure may be disabled by the Board's designee during use by an adult to enable access for bona fide research or other lawful purpose.

The District shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate, its initial Internet safety measures.

Specific expectations for appropriate Internet use shall be reflected in the District's code of acceptable behavior and discipline.

Access to Electronic Media

(Acceptable Use Policy)

RESTRICTIONS

The following restrictions against inappropriate speech and messages apply to all speech communicated and accessed through the District Internet system, including e-mail, instant messages, Web pages, and Web logs:

1. Students shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages.
2. Students shall not post information that could cause damage, danger, or substantial or material disruption or engage in personal attacks, including prejudicial or discriminatory attacks.
3. Students shall not harass another person or knowingly or recklessly post false or defamatory information about a person or organization.

PERMISSION/AGREEMENT FORM

A written parental request shall be required via Online Registration prior to the student being granted independent access to electronic media involving District technological resources. The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations, must be signed by the parent or legal guardian of minor students (those under 18 years of age) and also by the student.

This document shall be kept on file as a legal, binding document. In order to modify or rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the Superintendent with a written request.

EMPLOYEE USE

Employees are encouraged to use electronic mail and other District technology resources to promote student learning and communication with the home and education-related entities. If those resources are used, they shall be used for purposes directly related to work-related activities.

Technology-based materials, activities and communication tools shall be appropriate for and within the range of the knowledge, understanding, age and maturity of students with whom they are used.

District employees and activity sponsors may set up blogs and other social networking accounts using District resources and following District guidelines to promote communications with students, parents, and the community concerning school-related activities and for the purpose of supplementing classroom instruction.

Networking, communication and other options offering instructional benefits may be used for the purpose of supplementing classroom instruction and to promote communications with students and parents concerning school-related activities.

In order for District employees and activity sponsors to utilize a social networking site for instructional, administrative or other work-related communication purposes, they shall comply with the following:

1. They shall request prior permission from the Superintendent/designee.

Access to Electronic Media

(Acceptable Use Policy)

EMPLOYEE USE (CONTINUED)

2. If permission is granted, staff members will set up the site following any District guidelines developed by the Superintendent's designee.
3. Guidelines may specify whether access to the site must be given to school/District technology staff.
4. If written parental consent is not otherwise granted through AUP forms provided by the District, staff shall notify parents of the site and obtain written permission for students to become "friends" prior to the students being granted access. This permission shall be kept on file at the school as determined by the Principal.
5. Once the site has been created, the sponsoring staff member is responsible for the following:
    a. Monitoring and managing the site to promote safe and acceptable use; and
    b. Observing confidentiality restrictions concerning release of student information under state and federal law.

Staff members are discouraged from creating personal social networking sites to which they invite students to be friends. Employees taking such action do so at their own risk.

All employees shall be subject to disciplinary action if their conduct relating to use of technology or online resources violates this policy or other applicable policy, statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. Conduct in violation of this Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

DISREGARD OF RULES

Individuals who refuse to sign required acceptable use documents or who violate District rules governing the use of District technology shall be subject to loss or restriction of the privilege of using equipment, software, information access systems or other computing and telecommunications technologies.

Employees and students shall be subject to disciplinary action, up to and including termination (employees) and expulsion (students) for violating this policy and acceptable use rules and regulations established by the school or District.

RESPONSIBILITY FOR DAMAGES

Students or staff members who deface a District web site or otherwise make unauthorized changes to a web site shall be subject to disciplinary action, up to and including expulsion and termination, as appropriate.

Access to Electronic Media

(Acceptable Use Policy)

RESPONDING TO CONCERNS

School officials shall apply the same criterion of educational suitability used to review other educational resources when questions arise concerning access to specific databases or other electronic media.

AUDIT OF USE

Users with network access shall not utilize District resources to establish electronic mail accounts through third party providers or any other nonstandard electronic mail system.

The Superintendent/designee shall establish a process to determine whether the District's education technology is being used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that meets requirements of Kentucky Administrative Regulations and that blocks or filters Internet access for both minors and adults to certain visual depictions that are obscene, child pornography, or, with respect to computers with Internet access by minors, harmful to minors;
2. Maintaining and securing a usage log; and
3. Monitoring online activities of minors.

RETENTION OF RECORDS FOR E-RATE PARTICIPANTS

Following initial adoption, this policy and documentation of implementation shall be retained for at least ten (10) years after the last day of service in a particular funding year.

REFERENCES:

KRS 156.675; KRS 365.732; KRS 365.734
701 KAR 005:120
16 KAR 1:020 KAR 001:020 (Code of Ethics (Code of Ethics)
47 U.S.C. 254/Children's Internet Protection Act; 47 C.F.R. 54.520
Kentucky Education Technology System (KETS)
47 C.F.R. 54.516
15-ORD-190

RELATED POLICIES:

03.13214/03.23214; 03.1325/03.2325; 03.17/03.27
08.1353, 08.2322
09.14, 09.421, 09.422, 09.425, 09.426; 09.4261
10.5

Adopted/Amended: 8/20/2015
Order #: 61

Electronic Access/User Agreement Form

I. PURPOSE

The "Acceptable Use Policy" ("AUP") and this related procedure, set forth the standards governing Daviess County Public Schools ("DCPS") staff and students' use of the DCPS Electronic Network Related Technologies and Access ("DCPS Network") system. This procedure also sets forth the rules under which authorized users may continue their access to and use of these resources and promotes the ethical, legal, and school-related use of the DCPS Network compliance with the Children's Internet Protection Act of 1998. Personal electronic devices will be governed under this procedure when such devices are attached to the DCPS network.

Authorized use of information resources must be consistent with the educational purposes for which these resources have been provided. Use of the DCPS Network is a privilege that is provided to help authorized users complete and deliver educational obligations. The DCPS Network provides authorized users with the means for communicating effectively with schools, teachers, administrators, the public, other government entities, and educational experts. These resources should be used in a manner that both enhances students' educational experiences and complies with Board policy and procedures. DCPS students, through their use of the DCPS Network, will gain skills and expertise that prepare them for an increasingly technology-oriented society.

These procedures are written to support the Acceptable Use Policy and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. We recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions.

II. DEFINITIONS

A. Daviess County Public Schools' Electronic Network Related Technologies and Access ("DCPS Network") is the system of computers, phones, terminals, servers, databases, routers, hubs, switches and distance learning systems connected to the DCPS Network and the Internet.

B. Distance Learning Equipment is a means for providing meetings, educational or professional courseware and workshops utilizing video and/or audio conferencing equipment, and/or media management systems to distribute video to individual classrooms and offices in schools.

C. Electronic Mail (e-mail) consists of electronically transmitted information including any combinations of text, graphics, audio, pictorial, or other information created on or received by a computer application system and includes the transmission data, message text, and all attachments.

D. Internet is a worldwide telecommunications system that provides connectivity for myriads of other smaller networks.

Electronic Access/User Agreement Form

DEFINITIONS (CONTINUED)

E. Other Electronic Devices include, but are not limited to, telecommunication devices such as phones, pagers, eReaders, and personal digital assistants that may or may not be physically connected to the network infrastructure.

F. Password is a secret word or series of letters and numbers that must be used to gain access to an online service or the Internet or to modify certain software (such as parental controls).

G. Authorized Users are any students enrolled in any classes offered by DCPS or any staff members employed by DCPS.

H. Website is a collection of "pages" or files on the Internet that are linked together and managed by a company, institution or individual.

III. GENERAL PROVISIONS

A. AUTHORIZED USERS

All authorized users shall adhere to the provisions of this procedure as a condition for continued use of the DCPS Network. It is a general policy of DCPS to promote the use of computers in a manner that is responsible, legal and appropriate anytime there is a connection to the District's hardwired or wireless network.

Except in cases involving students who are eighteen (18) years of age or older, parents/guardians may request to review the contents of their child(ren)'s email files.

Parents/guardians wishing to challenge information accessed via the District's technology resources should refer to Policy 08.2322/Review of Instructional Materials and any related procedures.

B. DISCLAIMER

Pursuant to the Children's Internet Protection Act, DCPS uses filtering software to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations that contain millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals/Dating; Lingerie/Swimsuit; Racism/Hate; Tasteless; and Illegal/Questionable. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Authorized users accessing the Internet do so at their own risk. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and students and staff gain access to inappropriate and/or harmful material, the Board will not be liable. To minimize these risks, use of the DCPS Network is governed by the Acceptable Use Policy. If users are able to view questionable content, the website(s) in question should immediately be reported to appropriate school administration and/or the Computer Operations Manager.

Electronic Access/User Agreement Form

IV. TERMS AND CONDITIONS FOR USE OF THE DCPS NETWORK

A. ACCEPTABLE USES

DCPS staff and students may use the various resources provided by the DCPS Network to pursue educationally-related activities. Teachers and other staff should help guide students in their use of the DCPS Network so that students will learn how Internet resources such as discussion boards, instant messaging and chat rooms can provide valuable educational information from classrooms, schools, and other national and international sources. In addition to using the DCPS Network strictly for educational pursuits, students will be expected to follow generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in your messages to others.
2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
3. Keep personal information, including the logins, passwords, addresses, and telephone numbers of students or colleagues confidential.
4. Use these resources so as not to disrupt service to other student authorized users.
5. Do not upload, post, e-mail, transmit, or otherwise make available any content that is unlawful, dangerous or may cause a security risk.

B. UNACCEPTABLE USES

Improper use of the DCPS Network is prohibited. Actions that constitute unacceptable uses of the DCPS Network and are not specifically addressed elsewhere in this procedure include, but are not limited to:

1. Use of the DCPS Network for, or in support of, any illegal purposes.
2. Use of the DCPS Network for, or in support of, any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If an authorized user inadvertently accesses such information, s/he should immediately disclose the inadvertent access to a teacher or to the school Principal. This will protect the user against allegations of intentionally violating this procedure.
3. Use of the DCPS Network for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass or "stalk" another individual.
4. Non-educational uses of the DCPS Network including, but not limited to games, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers, religious activities or political lobbying.
5. Use of profanity, obscenity or language that is generally considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities.
6. Plagiarizing any information gained on or through use of the DCPS Network or any other network access provider.

Electronic Access/User Agreement Form

B. UNACCEPTABLE USES (continued)

7. Using copyrighted materials, including commercial software, without permission of the copyright holder, and in violation of state, federal or international copyright laws. (If students are unsure whether or not they are using materials in violation of copyright provisions, they should ask their teachers or a school technology coordinator for assistance. School-based personnel are encouraged to contact the Public Relations Department if they have questions regarding use of copyright materials found through the DCPS Network.)
8. Violating of any provisions of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99) which governs students' rights to privacy and the confidential maintenance of certain information including, but not limited to, a student's grades and test scores is prohibited.
9. Using the DCPS Network for personal financial gain or for the transaction of any business or commercial activities.

C. SECURITY

All authorized users are to report promptly any breaches of security violations of acceptable use and the transmission of web addresses or e-mail information containing inappropriate material (as outlined in Section III B) to appropriate school personnel. Authorized personnel will report such breaches to the Computer Operations Manager or Superintendent /designee. Failure to report any incident promptly may subject the authorized user to corrective action consistent with the school-based code of discipline or staff code of conduct, in conjunction with Board rules and policies.

In order to maintain the security of the DCPS System, students are prohibited from engaging in the following actions:

1. Connecting to any network other than the DCPS-provided network when available.
2. Intentionally disrupting the use of the DCPS Network for other users, including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, or engaging in “hacking” of any kind, which is an illegal or unlawful entry into an electronic system to gain unauthorized information.
3. Intentionally spreading computer viruses or programs that loop repeatedly, or for the purpose of infiltrating a network or computer system without authorization or for damaging or altering without authorization the software components of a network or computer system.
4. Exposing and/or disclosing the contents or existence of DCPS computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients. Authorized users must not share logins or password(s) and unauthorized information regarding other users' passwords or security systems.
5. Downloading/running games, programs, files, electronic media, and/or stand-alone applications from the Internet that may cause a threat to the DCPS Network and/or its performance.

Electronic Access/User Agreement Form

V. STUDENT EPUBLICATIONS

Student authorized users may electronically publish as a part of a class activity. Material presented on a student's class activity publication site must meet the educational objectives of the class activity. DCPS has the right to exercise control over the content and/or style of the student ePublications. Students must use their state-issued email address to authenticate any third party application, which allows publication of school-assigned material.

Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student ePublication shall be identified by first name only for confidentiality and safety purposes.

NOTE: If the recorded image, voice, or work of a student is to be included in a publication as part of a commercial or for-profit fund-raising endeavor, affirmative authorization of the parent/guardian or eligible student must be obtained. (See related procedure 09.14 AP.251)

VI. NO PRIVACY GUARANTEE

The Superintendent/designee has the right to access information, including phone recordings, stored in any user directory, on the current user screen, or in electronic mail. S/he may review files and communications to maintain system integrity and insure that individuals are using the system responsibly. Users should not expect files stored on District servers or information transmitted through District provided or sponsored technology services, to be private.

VII. ASSUMPTION OF RISK

DCPS will make a good faith effort to keep the DCPS Network system and its available information accurate. However, authorized users acknowledge that there is no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information available. For example, and without limitation, DCPS does not warrant that the DCPS Network will be error free or free of computer viruses. In making use of these resources, authorized users agree to release the Board from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the DCPS Network. Authorized users further acknowledge that the information available through interconnecting networks may be inaccurate. DCPS has no ability to maintain such information and has no authority over these materials. DCPS makes no warranty of any kind, either express or implied, regarding the accuracy, quality, or validity of the data and/or information residing on or passing through the DCPS Network from outside networks. Use of the DCPS Network is at the risk of the authorized user.

VIII. INDEMNIFICATION

The authorized user indemnifies and holds the Board harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the DCPS Network that cause direct or indirect damage to the user, DCPS, or third parties.

IX. SANCTIONS

Additional rules and regulations may be found in District handbooks and/or other documents. Violations of these rules and regulations may result in loss of access/usage as well as other disciplinary or legal action.

Electronic Access/User Agreement Form

As a user of the Daviess County Public School District's computer network, I hereby agree to comply with the District's Internet and electronic mail rules and to communicate over the network in a responsible manner while abiding by all relevant laws and restrictions. I further understand that violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action and/or legal action may be taken.

Formal consent and signatures are to be given by staff during annual training requirements and by parents/guardians and students during Online Registration.

PRIOR TO THE STUDENT'S BEING GRANTED INDEPENDENT ACCESS PRIVILEGES, THE FOLLOWING SECTION MUST BE COMPLETED FOR STUDENTS UNDER 18 YEARS OF AGE:

As the parent or legal guardian of the student (under 18) signing above, I grant permission for my child to access networked computer services such as electronic mail and the Internet. I understand that this access is designed for educational purposes; however, I also recognize that some materials on the Internet may be objectionable, and I accept responsibility for guidance of Internet use by setting and conveying standards for my child to follow when selecting, sharing, researching, or exploring electronic information and media.

CONSENT FOR USE

By signing this form, you hereby accept and agree that your child's rights to use the electronic resources provided by the District and/or the Kentucky Department of Education (KDE) are subject to the terms and conditions set forth in District policy/procedure. Please also be advised that data stored in relation to such services is managed by the District pursuant to policy 08.2323 and accompanying procedures. You also understand that the e-mail address provided to your child can also be used to access other electronic services or technologies that may or may not be sponsored by the District, which provide features such as online storage, online communications and collaborations, and instant messaging. Use of those services is subject to either standard consumer terms of use or a standard consent model. Data stored in those systems, where applicable, may be managed pursuant to the agreement between KDE and designated service providers or between the end user and the service provider. Before your child can use online services, he/she must accept the service agreement and, in certain cases, obtain your consent.

NOTE: FEDERAL LAW REQUIRES THE DISTRICT TO MONITOR ONLINE ACTIVITIES OF MINORS.

Review/Revised: 2/16/2023