Davis School District Policy and Procedures

Subject: 7SS-003 Technology Resources and Internet Safety
Index: Support Services
Revised: October 3, 2017

---

1. PURPOSE AND PHILOSOPHY

The Davis School District (the "District") provides a system of Technology Resources (the "System") for educational purposes including classroom activities, professional or career development, administration of programs, and limited high-quality personal research.

2. RESPONSIBILITIES

2.1. The Administrator of Technology Services will serve as the coordinator to oversee the System.

2.2. The school principal, or designee, will serve as the building-level coordinator for use of the System, at individual school sites and will:

2.2.1. approve building-level activities;
2.2.2. ensure employees receive proper training in the use of the System and the requirements of this policy;
2.2.3. establish procedures to ensure adequate training and supervision of students using the System;
2.2.4. require all employees and students utilizing the System sign the applicable Technology Resources Acceptable Use Agreement (AUA); and
2.2.5. interpret the AUA at the building-level.

2.3. The department director, or designee, will serve as the department-level coordinator for use of the System at district-level worksites and will:

2.3.1. approve department-level activities;
2.3.2. ensure employees receive proper training in use of the System and the requirements of this policy;
2.3.3. require all employees utilizing the System sign the applicable AUA; and
2.3.4. interpret the AUA at the department-level.

3. ACCEPTABLE USE AGREEMENTS

The District has created three Technology Resources Acceptable Use Agreements ("AUA"s), each targeted to a specific population of the school community. These include a Secondary Student Agreement, Elementary Student Agreement and an Employee Agreement. These AUAs express the terms and conditions for use of the System including District Internet access. Individuals may not be given access to the System until such time as they have agreed to and signed the applicable AUA.

3.1. Student Use. The District will notify parents about the District System and policies governing its use. Parents and students must sign the applicable AUA each school year in order for the student to access the System.

3.2. Employee and Board Member Use. District employees and Board Members must sign the applicable AUA upon initial hire or taking office and each school year thereafter in order to access the System.

4. INTERNET SAFETY

One component of the System is Internet access. The District provides Internet access to employees, Board members, students, and guests through an agreement with Utah Education Network (UEN).

4.1 Filtering.

4.1.1. Internet content filtering, also known as Internet Content Management, is provided for all District supplied Internet service in order to block access by users to visual depictions deemed to be "obscene," "child pornography," "harmful to minors," or otherwise inappropriate to the school environment.

4.1.2. The Administrator of Technology Resources may disable content filtering for adults engaged in bona fide research or other lawful activities.

4.2. Monitoring.

The District will monitor the online activities of users who access the Internet through the System.

4.3. Instruction and Supervision of Student Use.

Faculty and staff will educate and supervise students about appropriate online behavior, including:

4.3.1. interacting with other individuals on social networking websites, email, text-messaging, and in chat rooms;
4.3.2. cyber-bullying awareness and response;
4.3.3. unauthorized online access, including "hacking" and other unlawful activities; and
4.3.4. unauthorized disclosure, use, and dissemination of personal information.

5. SELECTION OF MATERIAL FOR CLASSROOM USE

When using District Technology Resources for educational activities, educators will:

5.1. Select material that is appropriate in light of the age of the students and relevant to the course objectives;

5.2. Preview the materials and sites they require students to access to determine the appropriateness of the material contained on or accessed through the site;

5.3. Provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly; and

5.4. Assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussion about controversial issues with the student and his or her parent.

6. INTERNET/INTRANET PUBLISHING

School and classroom web pages, virtual learning environments, blogs, podcasts, or other Web 2.0 tools are considered an extension of the school environment when originating from or being conducted through District System resources or are sponsored by District employees or groups.

All District sponsored material posted or published to the Internet or Intranet must comply with the Davis School District Internet/Intranet Publishing Guidelines as well as the Davis School District Social Media Guidelines.

6.1. School Web Pages

School Web Pages include the school's homepage as well as department, educator, club, team, group, or student web pages.

6.1.1 The building principal will designate a school web publisher, responsible for managing the school website and monitoring class, educator, student, and extracurricular web pages. All official material originating from the school will be consistent with the District style and content publishing guidelines and approved through a process established by the school web publisher.

6.1.2 The following minimum standards will be followed regarding the disclosure of student information on school web pages:

[a] Students' picture and name shall not appear on the same web page.
[b] Students' home address and phone number shall not be posted.
[c] Class rosters or student class schedules shall not be posted.

6.2. District Web Pages

A District department supervisor may designate a department web publisher responsible for managing the department's site. All official material originating from the department will be consistent with the District style and content publishing guidelines.

7. COLLECTION OF USER INFORMATION

If the District or an individual school collects personally identifiable information from users who access its website, the District or individual school shall publish on its website a privacy policy statement that discloses the following information:

7.1. the identity of the District's or school's Web publisher and contact information;

7.2. a summary of the personally identifiable information collected and contained on its website or servers;

7.3. how the personally identifiable information collected by the District or school is used by the District or school;

7.4. the District's or school's practice concerning disclosure of the personally identifiable information on the website;

7.5. how the user who accesses the District's or school's website can request access to his or her personally identifiable information and how the individual may request to correct the information; and

7.6. a general description of the security measures in place to protect the individual's personally identifiable information from unintended disclosure.

8. VIOLATIONS

8.1. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the System.

8.2. In the event there is an allegation that a student has violated this policy or the District AUA, the student will be provided with a notice and opportunity to be heard in the manner set forth in the student disciplinary policy.

Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network.

8.3. In the event there is an allegation that an employee has violated this policy or the District AUA, the matter will be handled in accordance with District policy, applicable negotiated agreement, and the law.

9. SEARCH AND SEIZURE

9.1. System users do not have an expectation of privacy in the contents of their System files and records or their online activity while on the District System.

9.2. Routine maintenance and monitoring of the System may lead to discovery that the user has violated or is violating this policy, District AUA, or the law.

9.3. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or District policy. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

10. COMPLAINT PROCEDURE

Complaints regarding this policy, its enforcement, or observed behavior shall be directed to the site administrator to investigate and resolve. The site administrator may seek assistance to resolve a complaint from appropriate district level administrators.

11. DISTRICT LIMITATION OF LIABILITY

The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District System will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the System. The District will not be responsible for financial obligations arising through the unauthorized use of the System. Users will indemnify and hold the District harmless from any losses sustained as the result of intentional misuse of the System by the user.

12. POLICY REVIEW AND DISSEMINATION

12.1. The Board shall review this policy at least every three (3) years.

12.2. Notice of the availability of this policy shall be posted in a conspicuous place within each school.

DEFINITIONS

"Child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct, and as further defined in section 2256 of Title 18, United States Code.

"Technology Resources System" or the **"System"** means the District's computer systems and networks including all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available.

"Harmful to minor" means that quality of any description or representation, in whatsoever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse when it: (1) taken as a whole, appeals to the prurient interest in sex of minors; (2) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and (3) taken as a whole, does not have serious value for minors. Serious value includes only serious literary, artistic, political or scientific value for minors.

"Personally identifiable information" means information that identifies 1) a user by name; account number; physical address; email address; telephone number; Social Security number; credit card information; or bank account information; 2) a user as having requested or obtained specific materials or services from a governmental website; 3) Internet sites visited by a user; or 4) any of the contents of a user's data-storage device. "User" in this definition means a person who accesses a governmental website.

"Obscene" has the meaning given such term in 18 U.S.C. 1460-1470.

REFERENCES

20 U.S.C. § 7001 – Children's Internet Protection Act (CIPA)
47 U.S.C § 254 – Schools and libraries to enact Internet Safety Policies.
Utah Code Ann. §§53A-3-422 to 423 – Internet and online access policy.
Utah Code Ann. Title 63D Chapter 2 – Governmental Internet Information Privacy Act
Utah Code Ann. §§76-10-1201 to 1206 – Pornographic and Harmful Materials and Performances
Utah Education Network 2-2, Network Acceptable Use Policy

FORMS AND OTHER LINKS

Elementary Student Acceptable Use Agreement
Secondary Student Acceptable Use Agreement
Employee Acceptable Use Agreement
Internet/Intranet Publishing Guidelines
Social Media Guidelines

DOCUMENT HISTORY:
Adopted: October 16, 2011
Revised: January 4, 2005 – 3 year review – Added acceptable use, selection of materials, web pages, collection of user information, due process and search and seizure sections.
Revised: May 15, 2012 – Updated policy to comply with changes in the Children Internet Protection Act (CIPA).
Revised: October 3, 2017 by consent - Five-year review. No substantive changes.