

Student Acceptable Use Agreement

Reasons for this Policy

A commitment to an exemplary student education in the 21st Century is at the core of Dry Creek Joint Elementary School District's various technology initiatives. While technology resources can enhance the students' learning and education when used for appropriate school purposes, it can distract and disrupt the process when it is abused. This Instructional Acceptable Use Policy (ITAUP) establishes the expectations to ensure District Technology (as defined below) is a valuable resource to students, rather than a hindrance to learning both on and off campus.

The access, use, and possession of District Technology is a privilege permitted at District's discretion and is subject to the conditions and restrictions set forth in applicable Board policies (e.g. Board Policy 6163.4) and this AUP. Network etiquette is explained below, which students are expected to follow. District reserves the right to suspend access to District Technology at any time, without notice, for any reason.

The purpose of this AUP is to ensure a safe and appropriate environment for all students. This AUP notifies parents and students about the acceptable ways in which District Technology may be used; it also notifies parents and students about the unacceptable use of District Technology.

Each student who is authorized to use District Technology, and his/her parent/guardian shall sign the AUP, below, as an indication that they have read, understood and agree to comply with the terms of this AUP.

Definitions

District Technology: The term "District Technology" shall collectively refer and relate to all District Devices (as defined below); District computer networks including servers and wireless computer networking technology (Wi-Fi); District User Accounts, (as defined below); District electronic devices such as USB drives, cameras, wireless access points (routers), District data networks, operating systems, storage, e-mail, systems, web applications, or mobile applications.

User Accounts: The term "User Account" shall refer and relate to a student's individual account on the *District* network server used to store student's computer username, password, and other information.

Device: The term "Device" or "Devices" is a subset of *District* Technology and shall specifically refer to a *District* -owned tablet, laptop or Chromebook to which the student has been given access and/or loaned to the student for educational purposes including but not limited to distance learning.

Student Obligations and Responsibilities

I. Acceptable Use of District Technology:

District students are only permitted to use District Technology for educational purposes which are safe (pose no risk to students, employees or assets), legal, ethical, do not conflict with the mission of District, and are compliant with all other District policies and regulations.

Acceptable use of District Technology includes use that is for the purpose of communicating between teachers and students, or between students for educational purposes.

2. Prohibited Use of District Technology:

Students are prohibited from using District Technology for improper purposes, including, but not limited to, using District Technology to:

- A. Violate any state or federal law or municipal ordinance including, but not limited to, the following:
 - Selling or purchasing any illegal substance;
 - Accessing, transmitting, or downloading child pornography, obscene depictions, harmful materials, or materials that encourage others to violate the law;
 - Transmitting or downloading confidential information or copyrighted materials;
 - Accessing, posting, displaying, or otherwise using material that is discriminatory, libelous, defamatory or disruptive;

INSTRUCTIONAL TECHNOLOGY ACCEPTABLE USE POLICY (ITAUP)

- Using District Technology to bully, harass, intimidate, or threaten other students, staff, or other individuals (“cyberbullying”);
 - Disclosing, using or disseminating personal identification information (such as name, address, telephone number, social security number, or other personal information) of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person;
- B. Access, transmit or download inappropriate matters on the Internet, as determined by the school board, local educational agency or other related authority.
- C. Obtain and/or use anonymous e-mail addresses.
- D. Cause harm to others or damage to their property including, but not limited to, the following:
- Deleting, copying, modifying, or forging other users' e-mails, files, or data;
 - Damaging computer equipment, files, data or the network;
 - Installing unauthorized software or applications;
 - Downloading large non-school related video, audio or other files;
 - Using profane, abusive or impolite language;
 - Disguising one's identity, impersonating other users or sending anonymous e-mail messages;
 - Threatening, harassing or making defamatory or false statements about others;
 - Accessing, transmitting or downloading offensive, harassing, or disparaging materials;
 - Accessing, transmitting or downloading computer viruses or other harmful files or programs, removing a computer program without permission from a teacher or other District personnel, changing settings on shared computers or in any way degrading or disrupting any computer system performance;
 - Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes"; or
 - Using any district computer to pursue hacking, internal or external to the district, or attempting to access information that is protected by privacy laws.
- E. Jeopardize access or lead to unauthorized access into User Accounts or other District computer networks including, but not limited to, the following:
- Using other students' User Account emails, passwords or identifiers;
 - Disclosing one's User Account password to other students or allowing other students to use one's User Account;
 - Getting unauthorized access into other User Accounts or other computer networks; or
 - Interfering with other students' ability to access their User Accounts.
 - Attempt to circumvent content filtering and internet security.
- F. Engage in commercial business, including but not limited to, the following:
- Selling or buying anything over the Internet for personal financial gain;
 - Using the Internet for advertising, promotion, or financial gain; or
 - Conducting for-profit business activities and engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for political purposes or soliciting votes.
- G. Using District Technology for non-educational purposes.
- H. Allow other persons to use District Technology, or login credentials without the express permission of the District.

3. No Expectation of Privacy Policy

Because the use of District Technology is intended for educational purposes, students shall not have any expectation of privacy in any use of District Technology. The System Administrator has the authority to monitor all User Accounts, including e-mail and other materials transmitted or received via the User Accounts, log files, browsing history, and other data about user activities with District Technology at any time, without prior notice. All such materials are the property of District.

4. Blocked or Restricted Access

Student access to specific Internet resources, or categories of Internet resources, deemed inappropriate or non-compliant with this AUA may be blocked or restricted based on District policies and educational mission. A particular web site that is deemed “acceptable” for use may, but not necessarily, be subject to blocking or restriction.

5. Personally Owned Devices

If a student uses a personally owned device to access District Technology, he/she shall abide by all applicable Board Policies and this AUA. Students may use personally owned devices for educational purposes and will be responsible for any fees charged by their personal device's service provider. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to be disclosed pursuant to a lawful subpoena or public records request.

6. District-owned Devices

If a student is using a District-owned device, he/she shall abide by all applicable Board Policies, the Device Use Agreement (below) and this AUP. Students may use District -owned devices for educational purposes only. Any use of a District-owned device may subject the contents of the device and any communications sent or received on the device to be disclosed pursuant to a lawful subpoena or public records request.

7. Reporting

If a student becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information), the damage or misuse of District Technology, he/she shall immediately report such information to the teacher or other District personnel.

8. Penalties for Improper Use

The use of the District Technology is a privilege, not a right; inappropriate use will result in the restriction or revocation of student's access to District Technology. Inappropriate use may lead to any disciplinary and/or legal action, including but not limited to suspension or expulsion or dismissal from District, or criminal prosecution by government authorities. District will attempt to tailor any disciplinary action to meet the specific concerns related to each violation.

9. District Rights and Disclaimers

- A. District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from the unauthorized use of District Technology. District also denies any responsibility for the accuracy or quality of the information obtained through District Technology.
- B. Any statement, accessible using District Technology, including advertisements on non- District web sites, is understood to be the author's individual point of view and not that of District, its affiliates or employees.
- C. Students are responsible for any losses sustained by District or its affiliates, resulting from the student's intentional misuse of District Technology.
- D. District reserves the right to restrict access to online destinations with network filters, software, or other means.
- E. District reserves the right to deny access to District Technology to any individual.
- F. Security on the network is a high priority. The Department of Technology shall establish procedures that will maximize system security.
- G. User Accounts which are inactive for more than 30 days may be removed by District along with the user's files without prior notice.
- H. School staff is responsible for supervising student use of District Technology on a District campus. Parents are responsible for supervising student use of District Technology when the students are not on campus.
- I. Illegal activities may be referred to the appropriate law enforcement agency.
- J. District reserves the right to revise and amend this AUP at any time.

For further information, please call the District (916)-770-8800.

INSTRUCTIONAL TECHNOLOGY ACCEPTABLE USE POLICY (ITAUP)

Acceptable Use Agreement

All parents or legal guardians of students under 18 must read and sign below. As the parent or legal guardian of the above student, I have read, understand and agree my child or dependent must comply with the provisions of the attached Acceptable Use Policy of the Dry Creek Joint Elementary School District. I give full permission to District to provide my child or dependent with access to District Technology including but not limited to the loan of a District-Chromebook or laptop for educational purposes including distance learning.

I accept full responsibility for the supervision of student's use of the District Technology including the District Chromebook or laptop and student's District User Account and the Internet at home or while not in a school setting. I understand and agree in the event a third party makes a claim against District as a result of my child or dependent's use of the District computer network, District, reserves its right to respond to such a claim as it sees fit and to hold all offending parties, including my child or dependent, responsible.

I release District, its affiliates and its employees from any claims or damages of any nature arising from my child or dependent's access or use of District Technology. I also agree not to hold District responsible for materials improperly acquired on the system, or for violations of copyright restrictions, users' mistakes or negligence, or any costs incurred by users.

This agreement shall be governed by and construed under the laws of the United States and the State of California.

School

Name of Student

Parent/Legal Guardian Name

Parent/Legal Guardian Signature Date

(Signed Electronically During Registration - DO NOT sign and return to school.)