Cardiff School District

Student Technology Acceptable Use Policy

Cardiff School District is pleased to offer all students access to a District-owned iPad as part of our One-to One (1:1) program to enhance all students' educational experience. All devices are owned by the District and are to be used for school-related work as a productivity and research tool as well as to promote school/home communication. These devices are intended only for the use of the student to whom it is assigned. It is not a replacement for personal technology devices and it is not intended for personal use.

Access to Cardiff School District technology resources (e.g., internal network and storage, Internet access, computers, iPads, etc.) will be provided to students who agree to use them in a responsible manner. To ensure proper use, the District may monitor usage of technology resources at any time without advance notice or consent. At the start of each school year and prior to being allowed access to the Internet at school, all students and their parent/guardian(s) must sign this document. In addition to this document, each teacher reviews the iPad Non-Negotiable rules with their class to reiterate important expectations when they use their assigned iPad. As Digital Age Learners, students must adhere to these agreements when using District technology resources.

Digital Citizenship

The International Society for Technology in Education (ISTE) Standards for Students are the foundation for teaching digital citizenship. These standards are the framework for students to engage and to act responsibly in a connected, digital world in safe, legal and ethical ways. For students who do not engage appropriately and responsibly, consequences of misuse will apply.

Common Sense Media curriculum is used in all classrooms to teach students the ISTE standards in order to develop good digital citizens by doing the following:

- Protect their own, and others, personal information and passwords
  Students should not post or transmit their own or other's personal information such as home addresses, telephone numbers, last names, photos, school of attendance, or other personal identifying information.

- Manage their digital footprint
  Students should manage their digital identity and reputation by being aware of how they represent themselves online. Students should not expect that files stored on or transmitted via the District's resources will be confidential. Teachers and administrators may review files and communications to maintain system integrity and ensure that students are using technology responsibly.

- Respect each other's ideas and opinions, and stand up to cyberbullying
  Students should not send, access, submit, publish, display or print over the Internet or District network any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive or illegal material. This includes taking photos or videos of students or staff without their permission.

- Properly cite resources from the Internet
  Students should adhere to all Copyright ©, Trademark TM, and/or Registered ®, laws. All materials from the Internet and other digital resources, including graphics, which are used in student projects or reports, must be properly cited.

- Adhere to Social Media Age Restrictions
  Students should not create or access social media websites if they are under the age of 13 unless permission is given by the parent/guardian(s).

Internet Access

Supervision and Monitoring - As required by the Children's Internet Protection Act, (CIPA), Cardiff School District provides students with a filtered and secure, protected environment within the District's network at each school site. When using technology in the classroom, staff will monitor and supervise Internet activity.

Filtering technology is not perfect and not all access to the Internet can be supervised during school hours, therefore some objectionable material may be viewed. Students are taught to immediately report unexpected, inappropriate content to their teacher or other staff member.

Any student who intentionally accesses inappropriate content on the Internet and/or loads apps, documents, content, images, or sound bytes onto their device will be dealt with in accordance with our District policies regarding student conduct.   Student personal email and other personal accounts should not be accessed with school devices.

Once the device leaves the District network, the filtering technology will still be implemented, however, it is the responsibility of the parent/guardian(s) to monitor student use of the device at home.

The device is configured for the District's wireless network. Internet access is available on the school site before, during and after school for all students. The district will not be able to assist families with connecting the device to home Internet providers.

District Subscriptions - The District offers individualized instruction to students through a variety of technological resources. In some instances, the District will offer educational websites or applications that utilize limited personal information of students, such as name, screen name, username, etc., in order to provide individualized instruction. Should such a website or application be utilized for educational purposes, it will be identified on the District website and families have the right to opt out of student use of such websites and applications. The District does not approve websites and applications that market or sell student personal information for commercial use.

Mobile Devices

The following applies to both SCHOOL and HOME use:

Apps - iPads are configured by the District's technology department with apps that are deemed appropriate by the teachers and/or administrators. Apps for personal use, such as games, entertainment, or social media, may not be installed on student iPads.

Off Campus Use - The iPad may be taken home outside of school hours by the student at the discretion of the classroom teacher. The student will be responsible to transport the iPad to and from school in a safe and secure manner. A cover is provided for the protection of the device and must be used at all times.

iPads must be at school during regularly scheduled school days in order to be utilized by the student in the classroom for accessing and completing school-related work.

Recording - Parents and students are not to audio, take photos, video record, or stream any virtual sessions or lessons. This includes lessons or instruction provided via telephone or a video conferencing platform.

Vandalism - Virtual and physical vandalism will not be tolerated. Any intentional act by a student that damages or interferes with the performance of District technology hardware, software, operating systems, and/or communication systems, will be considered vandalism and will be subject to school discipline and/or appropriate criminal or civil action. The student is financially responsible to replace the device due to any malicious damage.

Theft - It is the student's and parent/guardian's responsibility to take every precaution and action to prevent the loss, theft, or damage to the device. If the device is lost or stolen on school property, students are to report the incident immediately to the teacher, who will then report it to the school site principal.

For off-campus loss or theft, the device should also be reported to the local police department. A copy of the police report must be sent to the district within 48 hours of the discovery of the loss. The student/parent/guardian is financially responsible to replace the device should there be an off-campus loss or theft.

Replacements - Should a District-owned technology device require servicing that results in loss of access during school hours, a replacement will be issued. In case of off-campus loss or theft, a replacement will be issued for use during school hours. Once payment is received, the student can resume taking the iPad home.

Legal Issues and Laws

It is a felony to intentionally access any computer system or network for the purpose of devising or executing any scheme or artifice to defraud or extort or obtain money, property, or services with false or fraudulent intent, representation, or promises. It is also a felony to maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program or data. Anyone committing such acts may face police charges in addition to disciplinary action by the school district.

Consequences of Misuse and/or Violation of the Provision of this Agreement

Misuse of District technology resources may result in disciplinary action up to and including expulsion from the District. This Agreement shall be used in conjunction with Cardiff School District Board of Education policies, California Education Code, and other local, state and federal laws and regulations governing the applicable matter.

Examples of Misuse Violations:

- Removing or changing another user’s password or account
- Using an account you are not authorized to use
- Damaging or altering any files including the network system
- Intentionally damaging any District electronic device
- Taking unauthorized photos or videos of students or staff

Consequences of Misuse Violations may Include:

- Limited access to the iPad or denial of home use
- Suspension or revocation of Internet access, network privileges, and/or computer access
- School suspension or expulsion
- Legal action and prosecution by authorities

Limitation of Liability
Cardiff School District shall not be responsible for any damages suffered by the student, including those arising from service interruptions, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies is at the student’s own risk. The student and his/her parent/guardian(s) shall indemnify and hold Cardiff School District harmless from any losses sustained as the result of use or misuse of the District’s technology resources by the student.