BOARD OF TRUSTEES
CARSON CITY SCHOOL DISTRICT

REGULATION No. 218
PROGRAM

INTERNET SAFETY AND TECHNOLOGY: ACCEPTABLE AND RESPONSIBLE USE

Introduction

The District is committed to internet safety, and the Board of Trustees has adopted a Policy on Acceptable and Responsible Use (ARU) of Technology which is designed to prevent unauthorized access and other unlawful activities by users, prevent unauthorized disclosure of or access to sensitive information, and to comply with legislation including, but not limited to, the Children's Internet Protective Act ("CIPA"), Children's Online Privacy Protection Act ("COPPA") and Family Educational Rights and Privacy Act ("FERPA"). The District's technology, systems, and services shall be used in a responsible, ethical, and legal manner.

The ARU Policy applies when District technology, systems, and services are used on and off District property. Additionally, the ARU Policy applies when personal technology is used to access District technology, systems, and services, and when personal technology is used on District property.

Definitions

For the purpose of this Regulation the following terms are defined:

Information and Communications Technology – also known as ICT, include any devices, networks, software, systems, services, XaaS, and other technology that enable interaction with digital data, systems, and services.

XaaS - is a term that collectively refers to the delivery of everything as a service. It recognizes the vast number of products, tools, and technologies that vendors now deliver as a service over a network, typically the Internet. This includes, but not limited to, SaaS, PaaS, and IaaS.

User - includes anyone using District technology resources regardless of the physical location of the user.

School service provider – is an entity that operates a school service pursuant to a contract with the District.

Family Educational Rights and Privacy Act ("FERPA") - is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Children's Online Privacy and Protection Act ("COPPA") - is a federal law created to protect the privacy of children under 13.

Children's Internet Protection Act ("CIPA") – was enacted by Congress to address concerns about children's access to obscene or harmful content over the Internet.

Personally Identifiable Information ("PII") - includes but is not limited to: a student's name; the names of members of a student's family; a student's address; a students' social security number; a student's unique education identification number or biometric record, or other indirect identifiers such as a student's date of birth, place of birth, or mother's maiden name, and other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community who does not have personal knowledge of the relevant circumstances to identify a student.

Personal Technology – is any technology that is not owned by the District.

School Official – shall mean a teacher, school library media specialist, school administrator or designee.

Authorized Users

District technology, systems, and services may be used by authorized students, employees, and other persons approved by the Superintendent or designee, such as, but not limited to, consultants, legal counsel and contractors. All users must agree to follow the District's policies and procedures and sign or electronically agree to the District's ARU Policy prior to accessing or using District technology, systems, and services, unless excused by the Superintendent or designee.

Use of the District's technology, systems and services is a privilege, not a right and may be revoked at any time and for any reason without prior notification. No user will be given access to District technology, systems, or services if such user is considered a security risk by the Superintendent or designee.

Digital Citizenship (Internet Safety)

Digital Citizenship has been defined as "the norms of appropriate, responsible technology use." The District believes that digital citizenship skills have become essential, especially in schools like ours that are using technology to transform learning. It shall be the responsibility of all District staff members to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this Regulation and CIPA.

Monitoring

The District reserves the right to monitor, inspect, copy, review, edit, delete, and store, at any time, and without prior notice, any and all usage of District technology, systems, and services and any and all information transmitted, received, or stored in connection with such usage. All such information files shall be and remain the property of the District, and no user shall have any expectation of privacy regarding such usage.

Student use of the District network and Internet will be under the direction of a teacher and monitored as any other classroom activity. However, use outside of school is the responsibility of the parent/guardian and should be monitored.

Content Filtering
The District filters all Internet content both on and off campus for inappropriate materials with the exception of the Jim Randolph High Tech Center, which is managed by Western Nevada College ("WNC") and is not filtered by either the District or WNC.

Students are monitored and content is filtered as required by the CIPA. However, content filters are not foolproof, and the District cannot guarantee that users will never be able to access inappropriate content using District technology, systems, and services. Evading, disabling, or attempting to evade or disable a content filter installed by the District is prohibited.

General Warning; Individual Responsibility of Users
All users and in the case of minors, their parents or guardians, are advised that access to the computer network may include the potential for access to materials inappropriate for school-aged students and the workplace. Every user must take responsibility for his or her use of the District's technology, systems, and services and stay away from these sites.

All users using District technology, systems, and services are responsible for any activity that takes place on their accounts. If a user suspects a security risk or breach, the user MUST notify the District's Department of Innovation and Technology within 24 hours. Users must not show or identify the problem to peers.

Personal Safety
In using the computer network and Internet, users should not reveal personal information such as name, home address, or telephone number. Users should avoid using their surname or any other information which might allow a person to locate the user without first obtaining the permission of a school official. Users under age 18 should not arrange face-to-face meetings with anyone they "meet" on the computer network or Internet without consent of parents or guardians. Regardless of age, users should never agree to meet a person they have only communicated with on the Internet in a secluded place or private setting.

Illegal Activities
It is a violation of this Regulation to use District technology, systems, and services to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law, including the possession or distribution of obscene or pornographic materials is strictly prohibited.

Confidentiality of User Information
PII concerning students may not be disclosed or used in any way on the Internet without verifiable consent of a parent or guardian or, if the student is 18 or over, the permission of the student is obtained. Exceptions to this rule include, but are not limited to exceptions allowed by, FERPA, which permits the District to disclose PII under qualifying circumstances.

User Privacy

A user does not have a legal expectation of privacy while using District technology, systems, and services, including, but not limited to, voice mail, telecommunications, e-mail, network, Internet and communications accessed, sent, received or stored. By using the District's technology, systems, and services, all users are consenting to have their usage monitored by the District**.**

Electronic communications, downloaded material, and all data stored on District technology, systems, and services, including files deleted from a user's account, may be intercepted, accessed, monitored or searched by the Superintendent or designee at any time in the regular course of business. Such access may include, but is not limited to, verifying that users are complying with District policies and rules, and investigating potential misconduct. Any such search, access, or interception shall comply with all applicable laws. Users are required to return District technology upon demand, including, but not limited to, mobile phones, laptops, and tablets.

Personal Devices

If personal technology is used on District property, use of personal technology must be consistent with this Regulation. Network and Internet activity is monitored and recorded, and misuse of personal devices, on or off the District network while on District property, will be subject to normal disciplinary action.

Connecting unauthorized technology to the District network is prohibited. Unauthorized technology includes any technology that is not owned by the District. However, users, excluding students, are permitted to connect personal technology to the "CCSD Guest" network. Exceptions can be made at the discretion of the Department of Innovation and Technology.

Use of personal technology that interferes with District technology, systems, and services is prohibited from being used on District property. This includes, but is not limited to, wireless access points, printers, hot spots, routers, network switches, and servers.

District Owned Technology

District provided technology, including but not limited to, laptops computers, Chromebooks, and tablets are provided to facilitate teaching and learning, to aid in administrative duties, and to facilitate school communications. Usage must be consistent with these purposes.

- Each user is responsible for the care and security of district technology assigned to such user.
- District devices are configured for use on the District network. The District WILL NOT assist in connecting to home, other networks or personal peripherals.
- Users are responsible for the confidentiality and security of personally identifiable information and other sensitive data stored by such user.
- Verifiable consent must be obtained from the Department of Innovation and Technology to adjust or modify District technology.
- All service, repairs and upgrades to District technology shall be performed by the Department of Innovation and Technology or designee.

Damaged and Lost or Stolen Technology

The user is responsible at all times for damages incurred to technology beyond normal wear and tear. The Department of Innovation and Technology or designee will determine whether damages are normal wear and tear or from negligent or inappropriate use.

If a District device is stolen or damaged as a result of negligence or intentional misuse, the user will be responsible for repair or replacement costs.

Student:

- The District reserves the right to charge the student or parent(s) or guardian(s) up to the full cost for the repair or replacement of District technology when damage/loss occurs due to negligence or intentional misuse.
- If stolen, the incident must be reported to a school official. In addition, a police report must be filed.

Employee:

- Any costs associated with the repair or replacement of District technology as a result of user negligence will be withheld from the employee's paycheck. A payment plan may be arranged if needed.
- If stolen, the incident must be reported within 24 hours to the employee's supervisor, the Department of Innovation and Technology and a police report must be filed.

Student Technology Return

The District will collect and inspect student issued technology and accessories at the end of each school year. In addition, student issued technology and accessories (originally supplied) must be returned when requested or when students terminate enrollment or graduate. Students who are withdrawn, expelled, or terminate enrollment for any reason must return their student issued technology prior to the date of termination. Students who transfer schools within District must return their student issued technology prior to transfer. For information pertaining to Chromebooks please reference the student "Chromebook Handbook" which can be found on the District website: www.carsoncityschools.com .

Employee Technology Return

Year-round employees are not required to check-in District issued technology at the end of the school year. All other employees are required to check-in their District issued technology. School principals, site administrators, and supervisors, have the discretion to permit the continued use of District issued technology throughout the summer months. However, the Department of Innovation and Technology reserves the right to require the check-in of District issued technology at any time, and for any reason.

If an employee does not turn in District issued technology by the required date, the employee's paycheck or any monies owed to the employee by the District may be withheld until all District issued technology is returned.

Data Storage

Data shall be stored locally on the user's District issued device, on a District server, or in the user's District issued OneDrive or Google Drive. In addition, users may store data on systems and services provided by school service providers. Storing data in any other location is prohibited.

Warranties/Indemnification

The District makes no warranties of any kind, expressed or implied, for the technology resources, systems, and services that it provides. The District shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the use of District technology resources, systems, and services.

The District's technology, systems, and services are available on an "as is, as available" basis.

The District is not responsible for the loss of data, delays, non-deliveries or service interruptions. The District does not endorse the content nor guarantee the accuracy or quality of information obtained using District technology, systems, and services.

By using District technology, systems, and services, users are taking full responsibility for their use or in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the District and all its employees harmless from any and all loss, costs, claims, or damages resulting from the use of District provided technology, systems, and services, including but not limited to any fees or charges incurred through purchases of goods or services by the user.

Unauthorized Use

Unauthorized Use includes, but is not limited to:

1. The malicious attempt to vandalize, harm, or destroy information or technology, or the actual vandalism, destruction, or harm thereof, on any District technology, system, or service.
2. Unauthorized access or attempting to gain unauthorized access to District technology, systems, or services.
3. The improper accessing, transferring, or sharing of network resources or files of other users.
4. The placing, transmission, distribution, or deliberate access of obscene, abusive, racist, sexist or otherwise offensive, objectionable, or unlawful information or language on any District technology, system, or service.
5. The unauthorized use of any District technology, system, or service for commercial purposes, financial gain, personal business, or production of advertisements, business endorsements, religious or political lobbying or other reasons not pre-approved.
6. The selling or purchasing of goods and services without the prior approval of the appropriate administrator.
7. The incurring of any unauthorized costs of any nature chargeable to the District.
8. Sending messages to a large number of people, or sending a large number of messages to a single person, with the intent of annoying the recipient (s) or to interrupt the Network (spamming.)
9. Installing or downloading any unauthorized or unlicensed software or files.
10. Setting a BIOS menu password.

Compliance with Governing Law

In the event this Regulation or accompanying regulation does not address a provision in applicable state or federal law or is inconsistent with or in conflict with applicable state or federal law, the provisions of applicable state or federal law shall control.

Reference: NRS 201.235 through 201.254; NRS 388.121 through 388.145; NRS 389.520; NRS 393.160; Children's Internet Protection Act (CIPA); Children's Online Privacy Protection Act (COPPA); Family Educational Rights and Privacy Act (FERPA).

Adopted: September 9, 1997
Revised: March 20, 2002
December 14, 2010
May 12, 2015
April 12, 2016
June 27, 2017
July 23, 2019