Administrative Regulation 7211
Responsible Use and Internet Safety

Responsible Office(s): Office of Information Technology

PURPOSE

This Administrative Regulation establishes the guidelines and procedures related to the responsible use of technology and digital media within the Washoe County School District ("District" or "WCSD").

REGULATION

1. This administrative regulation:

    a. applies to all users of the District's network to include, but not limited to: students, staff, voluteers, student teachers, 3rd party consultants, and contractors; and

    b. applies to all systems and technology that are owned or leased by the District. District technology may include, but is not limited to: computer equipment; District-issued cell phones; software licensed to the District; operating systems; storage media; and network accounts which provide electronic mail, internet browsing, and file transfers. These systems are to be used for District business, research, and educational purposes in serving the interests of the District's students and staff in the course of normal operations.

2. Through this administrative regulation, the District seeks to:

    a. ensure the responsible use of technology and digital media, foster the development of responsible, ethical technology users, emphasize the educational and collaborative value of technology, and outline the expectations and responsibilities of all users of the District's network; and

    b. establish the criteria for the responsible use of technology and digital media to protect staff, students, volunteers and the District from inappropriate technology use, which may expose the District to various risks including malicious code attacks, compromise of network systems and services, and legal issues.

3. Responsible Use

    a. All users of District technology and digital media shall act safely, responsibly, and ethically at all times.

b. Through this regulation, the district seeks to emphasize the educational and collaborative value of technology, and outline the expectations and responsibilities of anyone using the District's technology resources.

c. Staff, students, volunteers and all other users shall be responsible for complying with the provisions of this document, as well as all other policies, regulations and rules of the District, when gaining access to the District's network, including the District's Guest Wireless Network. This includes the use of personal devices on District property or at a District-sponsored activity.

d. Individuals accessing District technologies should:

   i. report to staff any inappropriate use of the Internet or any destruction of District property;

   ii. Protect ones own password and ensure others do not access their accounts. This includes regularly changing ones password;

4. Prohibited Uses

   a. The District emphasizes responsible use of technology for educational and administrative functions. Prohibited uses of technology include, but are not limited to:

      i. any activity that is illegal under local, state, federal, or international law and/or prohibited under District policies and regulations;

      ii. using a WCSD technology resource to actively engage in procuring or transmitting material that is in violation of District policies and regulations and/or applicable state and federal laws and regulations, to include those related to bullying, cyber-bullying, harassment, discrimination or hostile work environment;

      iii. transmission of any communication where the meaning of the message or its transmission or distribution would violate any federal or state law, the acceptable use policies of public access networks, or District policies, administrative regulations and procedures;

      iv. connecting non-District devices or equipment to the District's wide-area network, or to local-area networks connected to the wide-area

network without prior written authorization from the Chief Information Officer;

v. using District technology resources for commercial purposes, without approval in accordance with District policies and regulations, including the advertising of commercial offerings and/or to conduct any outside business, publicize non-educational fund-raising opportunities, commercial advertising, misrepresentation, or fraudulent offers of products, items, or services;

vi. installation or use of any copyrighted software for which WCSD or the end user does not have an active license;

vii. any activity designed to or resulting in the introduction of malicious programs to District technology resources;

viii. effecting security breaches or any disruptions of network communication, including, but are not limited to, accessing data of which the employee is not an intended recipient, logging into a server or account that the employee is not expressly authorized to access;

ix. port scanning or security scanning, without written permission from the Office of Information Technology;

x. all forms of network monitoring which will intercept data not intended for the employee or student;

xi. circumventing user authentication or security of any host, network or account;

xii. interfering with or denying service to any other user's computer (for example, a denial of service attack); and

xiii. using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.

b. Certain employees are exempt from the stated prohibited uses for expressed purposes, and only during the course of their legitimate job responsibilities:

    i. Staff of the Office of Information Technology and other District staff specifically authorized by the Chief Information Officer, in the active and specific investigation of illegal activity or violation of District policy, or in the planning, development, and execution of technical and procedural safeguards;

    ii. Site administrators or their specifically authorized delegates acting with reasonable suspicion in the active and specific investigation of student illegal activity or violation of District policy; and

    iii. Designated officers of the District's School Police Department.

5. Student Behavioral Interventions

    a. Inappropriate use, damage, or loss of District technology resources by a student shall be approached through the use of positive behavioral interventions, with the objective to support students' responsible use of technology. Technology-related offenses shall be subject to the same progressive discipline procedures and positive behavioral interventions as any non-technology-related offense.

    b. Removal of a student's access to technology resources is not considered a positive behavioral intervention, and shall only be considered in extreme cases. Any removal of a student's access to technology resources shall be temporary and include a provision for the student to regain technology privileges within a reasonable time period.

    c. In the development of behavioral interventions, schools shall consider appropriate behavioral and educational supports for studens to learn the appropriate use of technology.

    d. Incidents of prohibited behavior, to include cyber-bullying, shall be dealt with in accordance with District policies and regulations, to include the Student Behavior Matrix.

e. As with any District property, the student, the student's parents/guardians, or both, may be held financially liable for any cost incurred to District technology resources through inappropriate use, damage, or loss. Unlawful activity may result in criminal prosecution.

6. Improper Use

   a. Improper use of the District's network, the District's Guest Wireless Network, and/or public access networks by a student or staff member may result in consequences including, but not limited to, a verbal warning, written reprimand, temporary or permanent loss of access privileges to the District and public access networks, or other consequences as deemed appropriate and in accordance with progressive discipline plans. Examples of improper use include, but are not limited to, the violation of federal or state law, the District's responsible use agreements, or District policies, administrative regulations, and procedures.

   b. The District retains the right to examine information or materials students and staff store on these networks and remove it if it causes undue congestion or interference with the work of others on the District's networks.

7. Disclaimer of Liability

   a. The District is not responsible for the improper use of public networks by students or staff.

   b. Students and staff are responsible for information they place on public networks accessed through the District's network as well as for information they find or take from public networks. Additionally, students and staff are responsible for determining if the information they find or place on public networks is appropriate for use in a school setting.

   c. The District is not responsible for information or services that are placed on public networks that may be objectionable to users of the network.

   d. The District is not responsible for damage that may occur from student or staff use of public networks including the loss of computer data, damage to computer data, computer viruses that may be acquired from a public network, or damages those viruses may cause.

e. The District makes no guarantees about the quality of services provided through District technology resources, and is not responsible for any claims, losses, damages, costs, or other obligations arising from the use of the District network or accounts.

f. Any additional charges a user accrues due to the use of the District network are to be borne by the user.

g. The District denies any responsibility for the accuracy or quality of the information obtained through user access.

h. The District denies any responsibility for material encountered on a computer network, including the Internet, which may be deemed objectionable to a user (or his/her parents, if a minor) or for any hostile or injurious actions of third parties encountered through a computer network.

i. Any statement accessible on the computer network or the Internet is understood to be the author's individual point of view and not that of the District, its affiliates or employees.

j. Due to the nature of electronic communications and changes in the law, it is impossible for the District to guarantee confidentiality of email sent and received over any computer network, or any information posted or retrieved using District technology.

DEFINITIONS

1. "Guest Wireless Network" refers to filtered and managed access to the Internet through District technology resources.

2. "Mobile Devices" refers to portable computing devices capable of connecting wirelessly to the Internet, including but not limited to laptops, tablets, and smartphones.

3. "Personal device" means any computer device, such as a laptop, tablet, or cellphone, capable of connecting, usually wirelessly, to the Internet, that is not owned by the District and is brought to a District location or used off-site to connect to District technology resources.

4. “Technology” refers to all District technology resources, including hardware, software, and services, whether on site or off site. Technology includes, but is not limited to, computer equipment and software, network equipment and software, services, including third party services, online educational services, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and file transfers.

DESIRED OUTCOMES

1. Through this administrative regulation, the District seeks to ensure the responsible use of technology and digital media through staff and student responsible use. Such use fosters the development of responsible, ethical technology users, emphasize the educational and collaborative value of technology, and outline the expectations and responsibilities of anyone using the District’s network.

IMPLEMENTATION GUIDELINES & ASSOCIATED DOCUMENTS

1. This document reflects the goals of the District’s Strategic Plan and aligns/complies with the governing documents of the District, to include:

    a. Board Policy 7200, 21st Century Learning and Digital Learning, and the associated administrative regulations

    b. Board Policy 5100, Student Behavior, and the associated administrative regulations

    c. Board Policy 9205, Safe and Respectful Learning Environment, and the associated administrative regulations

    d. Board Policy 9201, Bullying, Harassment and Disctimination Prohibited, and the associated administrative regulations

    e. Administrative Regulation 5007, Student E-Mail

    f. Administrative Regulation 7201, Digital Learning

    g. Administrative Regulation 7202, Internet Filtering, Monitoring, and Compliance

    h. Administrative Regulation 7203, Online Educational Services

    i. Administrative Regulation 7224, Guest Network Access

2. This document complies with Nevada state laws and regulations, to include:
    a. Nevada Revised Statutes (NRS)
        i. Chapter 201, and specifically:
            1. NRS 201.235-201.254, Obscenity.
        ii. Chapter 388, System of Public Instruction, and specifically:
            1. NRS 388.121 – 388.1459, Safe and Respectful Learning Environment
        iii. Chapter 388, System of Public Instruction, and specifically:
            1. NRS 388.134, Policy by school districts for provision of safe and respectful learning environment and policy for ethical, safe and secure use of computers; provision of training to board of trustees and school personnel; posting of policies on Internet website; annual review and update of policies
            2. NRS 388.271, Board of trustees and governing body to adopt policies and procedures governing use of certain software and manner in which data concerning pupils may be provided in certain circumstances
            3. NRS 388.272, Required provisions for contracts that provide for disclosure of data that includes personally identifiable information of a student
        iv. Chapter 389, Academics and Textbooks, and specifically:
            1. NRS 389.502, … establishment of policy for ethical, safe and secure use of computers
        v. Chapter 389, Examinations, Courses, Standards and Graduation, and specifically:
            1. 1. NRS 389.520, Council to Establish Academic Standards: Establishment of standards; periodic review of standards; adoption of standards by State Board; establishment of policy for ethical, safe and secure use of computers

3. This document complies with federal laws and regulations, and specifically:
    a. Children's Internet Protection Act: 20 U.S.C. 6801 and 47 U.S.C. 254(h).
    b. Broadband Data Improvement Act, Title II, Protecting Children in the 21st Century Act

REVIEW AND REVISION

1. This administrative regulation shall be reviewed as part of the bi-annual review and reporting process, following each regular session of the Nevada Legislature.
2. Additional administrative regulations and/or other associated documents may be developed as necessary to implement and support this document.

REVISION HISTORY

Date	Revision	Modification
09/26/1995	1.0	Adopted
01/22/2002	2.0	Revised
10/25/2011	3.0	Revised: pursuant to changes to NRS 388, Safe and Respectful Learning Environment
11/27/2017	4.0	Revised: merged with Administrative Regulation 6163.2; removed RU Agreement