Descriptor Term	Descriptor Code	Issues Date
INTRANET/INTERNET SAFETY POLICY	IJND/IJND-R	June 19, 2002
	Rescinds	Issued

PURPOSE

The purpose of this policy is to provide the procedures, rules and guidelines for use of the Deming Public Schools Intranet/Internet resources. Use of such technology is a necessary element of the Deming Public Schools educational mission, but is furnished to staff and students as a privilege, not a right. The Deming Public School District seeks to protect legitimate users of technology by establishing limits on such use and sanctions for those who abuse the privilege. Eliminating computer abuse provides more computing resources for users with legitimate needs.

DEFINITIONS

The definition of the Intranet is any configuration of hardware and software that connects users. The network includes all of the computer hardware, operating system software, application software, stored text and data files. This includes electronic mail, local databases, externally accessed databases, cd-rom, recorded magnetic or optical media, clip art, digital images, digitized information, communication technologies and new technologies as they become available. Stand-alone workstations are also governed by this policy. As used herein, the user shall mean the system operations, staff members, account holders, and authorized students afforded access and use of the school district computer systems as part of the school district curriculum.

The definition of the Internet is any method or equipment used to access resources on the World Wide Web.

INTRODUCTION

Deming Public Schools resources for teaching and learning, communication services, and business data services are provided through computer equipment and maintaining access to local, regional, national, and international sources of information. The school district permits use of it computer system and information resources by students and staff who must maintain respect for the public trust and through which they have been provided, in accordance with policy and procedures established by the school district. These procedures do not attempt to articulate all required or prescribed behavior by its users. Successful operation of the computer system and network requires that all users conduct themselves in a responsible, decent, ethical and polite manner while using the network. The user is ultimately responsible for his/her actions in accessing network services.

Descriptor Term	Descriptor Code	Issues Date
INTRANET/INTERNET SAFETY POLICY	IJND/IJND-R	June 19, 2002
	Rescinds	Issued

GUIDELINES

1. Access to the computer system, information networks and to the information technology environment within the School District's system is a privilege and must be treated as such by all users of the network and its associated systems.
2. The School District's system will be used solely for the purpose of research, education, and school related business and operations.
3. Any user account or password assigned by the School District for access to network resources such as Internet and email shall only be used by the authorized user. Account owners are ultimately responsible for all activity under their account and shall abide by the School District's Intranet/Internet Safety Policy.
4. All users must exercise prudence in the shared use of the network. The School District reserves the right to limit use of such resources if there are insufficient funds, accounts, storage, memory, or for other reasons deemed necessary by the system operators. Or if an individual user is determined to be acting in an irresponsible or unlawful manner.
5. All communications and information accessible and accessed via the School District's system are and shall remain the property of the School District.
6. Student use shall be supervised and monitored by system operators and authorized staff and shall be related to the School District curriculum.
7. Any defects or suspected abuse in system accounting, security, hardware or software, shall be reported to the system operators.

UNACCEPTABLE USE

The Deming Public School District has the right to take disciplinary action, remove computer and networking privileges, or take legal action or report to proper authorities, any activity characterized as unethical, unacceptable or unlawful. Unacceptable use activities constitute, but are not limited to, any activity through which any user:

1. Violates such matters as institutional or third party copyright, license agreements or other contracts. The unauthorized use, copying or installation of software is illegal.
2. Interferes with or disrupts other network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses or worms, distributing quantities of information that overwhelm the system (chain letters, network games, etc.) and/or using the network to make unauthorized entry into any other resources accessible via the network.

3. Seeks to gain or gains unauthorized access to information resources, obtains copies of or modifies files or other data, or gains and communicates passwords belonging to other users.

4. Uses or knowingly allows another to use any computer, computer network, computer system, program, or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations.

5. Destroys, alters, dismantles, disfigures, prevents rightful access to, or otherwise interferes with the integrity of computer based information resources, whether on stand alone or networked computers.

6. Invades the privacy of individuals or entities.

7. Uses the network for commercial or political activity or personal or private gain.

8. Uses the School District system to compromise its integrity (hacking software) or accesses, modifies, obtains copies of or alters restricted or confidential records or files.

9. Submits, publishes or displays any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private.

10. Use of the School District system for illegal, harassing, vandalizing, inappropriate, or obscene purposes, or in support of such activities is prohibited. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Harassment is defined as slurs, comments, jokes, innuendos, unwelcome compliments, cartoons, pranks, and/or other verbal conduct relating to an individual which: (a) has the purpose or effect of creating an intimidating, hostile or offensive environment; (b) has the purpose of effect of unreasonably interfering with an individual's work or school performance; or (c) interferes with school operations. (see NMSA 1978, § 30-45-1 et.seq.) Vandalism is defined as any attempt to harm or destroy the operating system, application software or data. Inappropriate use shall be defined as a violation of the purpose and goal of the network. Obscene activities shall be defined as a violation of generally accepted social standards in the community of use of a publicly owned and operated communication device.

Descriptor Term	Descriptor Code	Issues Date
INTRANET/INTERNET SAFETY POLICY	IJND/IJND-R	June 19, 2002
	Rescinds	Issued

USER CODE OF CONDUCT

1. Keep confidential and protect all computer and Internet passwords, access codes or logon information from disclosure to others.
2. Respect the privacy of other users. Do not use other users' passwords. Unauthorized use of passwords, access codes or other confidential account information may subject the user(s) to discipline, and to both civil and criminal liability.
3. Be ethical and courteous. Do not send hate, harassing or obscene mail, discriminatory remarks, or demonstrate other anti-social behaviors. State law prohibits the use of electronic communication facilities to send fraudulent, harassing, obscene, indecent, profane, intimidating or other unlawful messages.
4. When sending email intended to boost morale (ie. educationally related joke or inspirational message) do not send to ALL DPS users. Choose the recipients whom you know will not be offended or irritated by your email. Any recipient who receives an email that he/she finds offensive has the obligation to notify the sender and request that no further emails of that nature be sent. No employee will be subject to discipline unless he/she repeats the act of sending inappropriate email to a recipient who has notified him/her as stated above.
5. Maintain the integrity of files and data. Do not modify or copy files/data of other users without their consent.
6. Treat information created by others as the private property of the creator. Respect copyrights. Software protected by copyright shall not be copied except as licensed and stipulated by the copyright owner.
7. Use the network in a way that does not disrupt its use by others. Do not use the Internet for commercial purposes. Transmission of commercial or personal advertisements, solicitations, promotions, destructive programs or other unauthorized use unrelated to the mission or curriculum of the school district is prohibited.
8. Do not destroy, modify or abuse the hardware or software in any way. Users shall report any suspected abuse, damage to equipment or tampering with files to the school district system operators.
9. Do not develop or pass on programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer of computing system, such as viruses worms, chain messages global mailings, etc. Do not "hack" the system. Attempts to gain unauthorized access to confidential information or private directories maintained by the school district or to circumvent privacy protections on internal files or non-public restricted files, accounts or directories of any external source is a violation of this code of conduct. And may subject the user to civil or criminal liability.

10. Do not use the Internet to view, access, download or process pornographic, obscene, indecent, profane or otherwise inappropriate material.
11. Use of the system to access games and use of computer time for game-playing shall be restricted solely to instances directed and monitored by instructional staff and is limited to games which address educational goals.

DEMING PUBLIC SCHOOL DISTRICT'S RIGHTS AND RESPONSIBILITIES

1. Monitor all activity on the School District's system.
2. Determine whether specific uses of the network are consistent with this policy.
3. Remove a user's access to the network at any time it is determined that the user is engaged in unauthorized activity or violating the Intranet/Internet Safety Policy.
4. Respect the privacy of individual user electronic data. The school district will secure the consent of user before accessing their data, unless required to do so by law or policies of the Deming Public School District.
5. Take prudent steps to develop, implement and maintain security procedures to ensure the integrity of individual and district files. However, information on any computer system cannot be guaranteed to be inaccessible by other users.
6. Attempt to provide error free and dependable access to technology resources associated with the School District system. However, the district cannot be held liable for any information that may be lost, damaged, or unavailable due to technical or other difficulties.
7. Provide an Internet filtering technology that protects users from receiving unsolicited inappropriate material via the district network.
8. Ensure that all student users complete and sign an agreement to abide by the district's Intranet/Internet Safety Policy. All such agreements will be maintained on file in the school office.

Descriptor Term	Descriptor Code	Issues Date
INTRANET/INTERNET SAFETY POLICY	IJND/IJND-R	June 19, 2002
	Rescinds	Issued

VIOLATIONS/CONSEQUENCES

1. Students:
   a. Students who violate this policy shall be subject to revocation of district system access up to and including permanent loss of privileges, and discipline up to and including expulsion.
   b. Violations of law will be reported to law enforcement officials.
   c. Disciplinary action may be appealed by parents and/or students in accordance with existing district procedures for suspension or revocation of student privileges.

2. Staff:
   a. Staff who violate this policy shall be subject to discipline, up to and including suspension, termination or discharge, in accordance with Board policy, negotiated agreements and applicable law.
   b. Violations of law will be reported to law enforcement officials.