Technology Policies for Students/Staff
of
Ganado Unified School District

I-6300 IJND TECHNOLOGY RESOURCES (Movies/Videos/Electronic Materials)

It is the policy of the District that there is educational value in utilizing movies and videos in classrooms only when such movies and videos extend and/or reinforce the concepts being taught and have been planned for in advance. Parents or guardians of students enrolled in the District shall have access in advance to instructional materials, learning materials and activities currently in use, or being considered for use, in the District.

The District shall obtain signed, written consent from a student's parent or guardian before using video, audio or electronic materials that may be inappropriate for the age of the student.

The Superintendent shall develop regulations governing the use of movies/videos in the classroom.

I-6311 IJND-R TECHNOLOGY RESOURCES (Movies/Videos/Electronic Materials)

Movies, videos and electronic materials with ratings other than for general audiences of all ages are not to be shown in classrooms or at any District facility (this includes buses and motels where students are present) except when:

- The movie, video or electronic material has been previewed by the teacher or other certificated staff member.
- The movie, video or electronic material has been determined to not contain material that is objectionable or inappropriate for the age group to which it is intended to be shown.
- The responsible school administrator has approved the use of the movie, video or electronic material prior to its showing.
- The teacher or other certificated staff member has provided advance notification to each student's parent(s), or other responsible adult, of the title of the movie, video or electronic material and the date on which it will be shown.
- When a movie, video or electronic material has a rating the above advance notification will include the rating and the source providing the rating.
- A student whose parent(s) or other responsible adult has provided notice of their disapproval will not be permitted to view the movie, video or electronic material.

Parents or guardians have the right to have advance access to instructional materials, learning materials and activities currently in use, or being considered for use, in the District.

Parents have the right to request that their child not view any movie or video, regardless of its rating or the purpose for which it is to be shown.

A parent or guardian who objects to any learning material or activity on the basis that it is harmful includes objection to a material or activity because it questions beliefs or practices in sex, morality, or religion or, because of sexual content, violent content, or profane or vulgar language, may request to withdraw that student from the activity or from the class or program in which the material is used and request an alternative assignment.

I-6400 IJNDB USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Appropriate use of Electronic Information Services

The District may provide electronic information services (EIS) to qualified students, teachers, and other personnel who attend or who are employed by the District. Electronic information services include networks (e.g., LAN, WAN, Internet), databases, and any computer-accessible source of information, whether from hard drives, tapes, compact disks (CDs), floppy disks, or other electronic sources. The use of the services shall be in support of education, research, and the educational goals of the District. To assure that the EIS is used in an appropriate manner and for the educational purposes intended, the District will require anyone who uses the EIS to follow its guidelines and procedures for appropriate use. Anyone who misuses, abuses, or chooses not to follow the EIS guidelines and procedures will be denied access to the District's EIS and may be subject to disciplinary and/or legal action.

The Superintendent shall determine steps, including the use of an Internet filtering mechanism, that must be taken to promote the safety and security of the use of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Technology protection measures shall protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to use of computers by minors, harmful to minors. Safety and security mechanisms shall include online monitoring activities.

As required by the Children's Internet Protection Act, the prevention of inappropriate network usage includes unauthorized access, including "hacking," and other unlawful activities; unauthorized disclosure, use and dissemination of personal identification information regarding minors.

It is the policy of the Board to:

- prevent user access over the District's computer network, or transmissions of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
- prevent unauthorized access and other unlawful online activity;
- prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
- comply with the Children's Internet Protection Act [P.L. No. 106-554 and 47 U.S.C. 254(h)].

Each user will be required to sign an EIS user's agreement. The District may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences. The District reserves the right to establish rules and regulations as necessary for the efficient operation of the electronic information services.

The District does not assume liability for information retrieved via EIS, nor does it assume any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

Filtering and Internet Safety

As required by the Children's Internet Protection Act, the District shall provide for technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by students, harmful to students. The protective measures shall also include monitoring the online activities of students.

Limits, controls, and prohibitions shall be placed on student:

- Access to inappropriate matter.
- Safety and security in direct electronic communications.
- Unauthorized online access or activities.
- Unauthorized disclosure, use and dissemination of personal information.

Education, Supervision and Monitoring

It shall be the responsibility of all District employees to be knowledgeable of the Board's policies and administrative guidelines and procedures. Further, it shall be the responsibility of all employees, to the extent prudent to an individual's assignment to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The Superintendent shall provide for appropriate training for District employees and for students who use the District's computer network and have access to the Internet. Training provided shall be designed to promote the District's commitment to:

- the standards and acceptable use of the District's network and Internet services as set forth in District policy;
- student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social networking Web sites, online opportunities and chat rooms; and cyberbullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act.

While training will be subsequently provided to employees under this policy, the requirements of the policy are effective immediately. Employees will be held to strict compliance with the requirements of the policy and the accompanying regulation, regardless of whether training has been given.

The Superintendent is responsible for the implementation of this policy and for establishing and enforcing the District's electronic information services guidelines and procedures for appropriate technology protection measures (filters), monitoring, and use.

I-6411 IJNDB-R REGULATION USE OF TECHNOLOGY RESOURCES IN INSTRUCTION (Appropriate Use of Electronic Information Services)

Acceptable use of the electronic information services (EIS) requires that the use of the resources be in accordance with the following guidelines and support the education, research, and educational goals of the District. The user must:

- Use the EIS for educational purposes only.
- Agree not to submit, publish, display, or retrieve any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
- Abide by all copyright regulations.
- Not reveal home addresses or personal phone numbers.
- Understand that electronic mail is not private.
- Not use the network in any way that would disrupt the use of the network by others.
- Understand that many services and products are available for a fee and acknowledge the responsibility for any expenses incurred without district authorization.
- Not use the EIS for commercial purposes.
- Follow the District's code of conduct.
- Not attempt to harm, modify, or destroy software or interfere with system security.

In addition, acceptable use for District employees is extended to include requirements to:

- Maintain supervision of students using the EIS.
- Agree to directly log on and supervise the account activity when allowing others to use a personal account.
- Take responsibility for personal accounts, including password protection.
- Take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of personal accounts by unauthorized persons.

Each user will be required to sign an EIS user's agreement. A user who violates the provisions of the agreement will be denied access to the information services and may be subject to disciplinary action. The District may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences.

Details of the user agreement shall have been discussed with each potential user of the electronic information services. When the signed agreement is returned to the school, the user may be permitted use of EIS resources through the school equipment.

I-6431 IJNDB-EA EXHIBIT USE OF TECHNOLOGY RESOURCES IN INSTRUCTION USE OF COMPUTERS, THE INTERNET, AND ELECTRONIC MAIL AGREEMENT AND PERMISSION FORM

The Ganado Unified School District No. 20 (hereinafter referred to as School) is pleased to offer students and staff (hereinafter jointly referred to as Users) access to a computer network for electronic mail and the Internet. To gain access to e-mail and the Internet, all Users must sign this Agreement and students must obtain parental permission as verified by the signatures on the form below. Should a parent prefer that a student not have e-mail and Internet access, use of the computers is still possible for more traditional purposes such as word processing.

What is Possible?

Access to e-mail and the Internet will enable staff and students to explore thousands of libraries, databases, museums, and other repositories of information and to exchange personal communication with other Internet users around the world. Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive. While the purposes of the School are to use Internet resources for constructive educational goals, Users may find ways to access other materials. The School believes that the benefits to students from access to the Internet in the form of information resources and opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Therefore, the School supports and respects each family's right to decide whether or not to apply for access.

What is Expected?
Users are responsible for appropriate behavior on the School's computer network just as they are in their work, classroom, or on the school playground. Communications on the network are often public in nature. General School rules for behavior and communications apply. It is expected that Users will comply with School standards and the specific rules set forth below. The use of the network is a privilege, not a right, and may be revoked and further disciplinary action may be taken if abused. The User is personally responsible for his/her actions in accessing and utilizing the School's computer resources. The Users are advised never to access, keep, or send anything that they would not want their supervisors, parents, or teachers to see.

General Conditions for Use
Privacy. Network storage areas may be treated like School lockers. Network administrators may review communications to maintain system integrity and ensure that Users are using the system responsibly and within the School's policies and guidelines.

Storage capacity. Users are expected to remain within allocated disk space and delete e-mail or other material which take up excessive storage space.

Illegal copying. Users should never download or install any commercial software, shareware, or freeware onto network drives or disks, unless they have written permission from the network administrator. Nor should students copy other people's work or intrude into other people's files.

Inappropriate materials or language. No profane, abusive, or impolite language should be used to communicate not should materials be accessed which are not consistent with the rules of School behavior. A good rule to follow is never view, send, or access materials which you would not want your supervisors, teachers, and parents to see. Should Users encounter such material by accident, they should report it to the network administrator or their teacher immediately.

Rules for Usage
These are rules and guidelines to follow to prevent the loss of network privileges and/or disciplinary action.

- Do not use a computer to harm other people or their work.
- Do not damage the computer or the network in any way.
- Do not interfere with the operation of the network by install ing illegal software, shareware, or freeware.
- Do not violate copyright laws. Copyrighted material may not be placed on the system without the express permission of the author who must be credited for the material. Copyrighted material may be downloaded for a User's use only.
- Do not view, send, or display offensive messages or pictures.
- Do not share your password with another person.
- Do not waste limited resources such as disk space or printing capacity.
- Do not trespass in another's folders, work, or files.
- Adhere to the rules of Internet etiquette set forth in the School's Internet policy.
- Read and adhere to the School's Internet policy attached hereto.
- Do not reveal your home addresses or personal telephone number or the addresses and telephone numbers of students, staff, or colleagues.
- Do notify an adult immediately if, by accident, you encounter materials which violate the Rules of Appropriate Use.
- Be prepared to be held accountable for your actions and for the loss of privileges and disciplinary action if the Rules of Appropriate Use are violated.