

Instruction

USE OF TECHNOLOGY IN INSTRUCTION

Copyrights

Users shall strictly observe copyright laws. All employees shall ensure that software is used and duplicated in accordance with software licensing agreements. Public domain software may be duplicated and exchanged with other schools or staff. No illegal copies of copyrighted software shall be accepted or used in the district.

(cf. 6162.6 - Use of Copyrighted Materials)

Selection of Educational Software

Before ordering software, the Technology Services *Computer Equipment and Software Standards List/Price List* should be consulted - <http://intranet.egusd.net/pricelist/> - to see if the software is pre-authorized. For educational software that is not on the list, staff should visit the California Learning Resource Network (CLRN) website - <http://clrn.org> – to see if the software has been reviewed and approved. All electronic resources approved by CLRN are reviewed using the California State Board of Education’s three-fold criteria:

- Legal Compliance Review
- Curriculum Frameworks and Standards Alignment Match Verification
- CLRN Minimum Requirements Review*

* CLRN Minimum Requirements:

1. The resource addresses standards as evidenced in the standards match and provides for a systematic approach to the teaching of the standard(s), and contains no material contrary to any of the other California student content standards.
2. Instructional activities (sequences) are linked to the stated objectives for this ELR (electronic learning resource).
3. Reading and/or vocabulary levels are commensurate with the skill levels of intended learners.
4. The ELR exhibits correct spelling, punctuation, and grammar, unless a primary source document.
5. Content is current, accurate and scholarly, including that taken from other subject areas.
6. The presentation of instructional content must be enhanced and clarified by the use of technology through approaches which may include: access to real-world situations (graphics, video, audio); multi-sensory representations (auditory, graphic, text); independent opportunities for skill mastery; collaborative activities and communication; access to concepts through hypertext, interactivity, or customization features; use of the tools of scholarship (research, experimentation, problem solving); simulated laboratory situations.

7. The resource is user friendly as evidenced by the use of features such as: effective help functions; clear instructions; consistent interface; intuitive navigational links.
8. Documentation and instruction on how to install and operate the ELR are provided and are clear and easy to use.
9. The model lesson/unit plan demonstrates effective use of the ELR in an instructional setting.

To order software *not* listed on the Technology Services *Computer Equipment and Software Standards List/Price List*, staff must complete the *EGUSD Software Request Form* and email, fax or mail it, along with any maintenance support documentation (if applicable) to Technology Services. For software listed on the CLRN website, simply note that on the form. The software will then be added to the standards list/price list.

Additional selection criteria for all software:

1. If the software is not in use in the district or is a new version of software that is in use in the district, the software will need to be tested by Technology Services on the EGUSD network prior to purchase to make sure it will work within the standards and constraints of the environment. Please allow 2-3 weeks for the testing process.

Instruction

USE OF TECHNOLOGY IN INSTRUCTION cont'd

INTERNET Use

The following terms and conditions shall be adhered to when staff and students use the district network and/or the INTERNET on district computers or via the district network:

The term INTERNET as used in this document refers to the public Internet, including, but not limited to, the World Wide Web, web pages, web logs (blogs), instant messaging, discussion boards, chat rooms, and other online learning communities and/or portals.

The term Web Page is defined as an actual HTML page, blog page, portal entry, or other representation/depiction on the Internet.

The term district network as used in this document refers to any connection made to the district network either via physical connection or wireless connection. The term password as used in this document refers to any password or password device that may be used to generate a onetime password, used to access the network or any network device or application.

1. Users who want to access the INTERNET must complete the [Application for Educational Use of the INTERNET](#). Students must complete the form annually.
2. The district makes no guarantees of any kind, whether expressed or implied, for the service it is providing. The district will not be responsible for any damages suffered by a user and makes no guarantee of access to sites. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the INTERNET is at the user's risk.
3. Users of the district network and/or INTERNET have a responsibility to assist in maintaining the security of the network. Therefore, users shall adhere to the following security regulations:
 - Users shall only use accounts assigned to them.
 - Users shall not attempt to log-in to accounts or systems for which they do not have authorized access.
 - Users must protect their password. Users should change their password periodically.
 - Users shall not use non-district computers, network devices or printers on the network without written authorization from Technology Services.

- Users shall maintain their password(s) as confidential. Users shall not give their password to anyone. This includes, but is not limited to, students, TA's, Technology Services, colleagues, and administrators.
- Users shall memorize their password.
- Users shall not write their password on a sticky note or piece of paper where it can be found. This includes: Hiding it under their keyboard or placing it on their monitor or in their desk drawer.
- Users shall lock the workstation or log out before leaving.
- Users shall not leave their computer unlocked when they are out of the room.
- Users shall log out if someone else needs to use the computer – they will have them login using their own username and password.
- Users shall not leave their workstation unattended while they are logged on.
- Users shall use the password feature of their screen saver.
- Users shall not allow anyone to use their email account to send email.
- Users shall not allow anyone to use their system accounts to work. If a person does not have the proper capabilities to do a task, he/she should contact Technology Services so the appropriate capabilities can be provided.
- Users shall not plug in wireless access points or anything into the network unless approved and authorized by Technology Services.
- Users shall not download confidential student or employee information onto laptops, desktops or other portable storage devices without authorization from the Director of Technology Services or designee. Authorized loading of confidential information onto laptops or other portable storage devices should only be done utilizing secure encryption.

5. Acceptable Use - The INTERNET including, but not limited to, the World Wide Web, blogs, discussion boards, chat rooms, and other online learning communities and/or portals is intended to be used in support of, and be consistent with, the educational standards and benchmarks of the district. Users will be provided access to the INTERNET in accordance with the District INTERNET filtering and blocking measures. These measures are in place to avoid access to inappropriate material that is not consistent with the educational standards and benchmarks of the district. Student access to INTERNET services is provided under staff supervision.

6. Unacceptable Use - The transmission or reception of any material in violation of any applicable laws, regulations, or district policies is prohibited. This includes but is not limited to, the misuse of copyrighted material or material protected by trade secret. Any transmission or reception of material by a student that is obscene, libelous, slanderous, gang-related, or incites students and/or staff so as to create a clear and present danger of: a) the commission of unlawful acts on school premises, b) the violation of lawful school regulations, or c) the substantial disruption of the orderly operation of the school, is prohibited and shall result in the termination of a user's INTERNET privileges and/or appropriate disciplinary actions. Prohibited "gang-related" materials are further described in BP/AR 5131.

- Malicious use of the District's systems or technology resources to develop or use programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
- Use of the network or personal electronic devices while on District property or during District sponsored events to intentionally access or process pornographic or adult sites with explicit sexual content or other inappropriate or derogatory material, inappropriate texting or messaging, or files dangerous to the integrity of the local area network is prohibited.
- The Elk Grove Unified School District network may not be used for downloading entertainment software, music, videos or other files not related to the mission and objectives of the Elk Grove Unified School District. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the Elk Grove Unified School District.

7. Privileges - The use of information technology is a privilege, and unacceptable use by students, as described in number six above, shall result in the cancellation of those privileges and/or appropriate disciplinary actions. The system administrator may close an account at any time as required. The principal/designee of any school may request the system administrator deny, revoke, or suspend a user's account.

8) Network Etiquette - Users are expected to abide by the generally accepted guidelines of network etiquette. These include (but are not limited to) the following:

- Users shall be polite, respectful and brief. Sarcasm, humor and using all caps may be misinterpreted as being rude.
- Users under age 18 shall not reveal their last names, addresses or phone numbers.
- Electronic mail (e-mail) is not guaranteed to be private and users acknowledge that they have no expectation of privacy. E-mail messages related to or in support of illegal activities shall be reported to an administrator who shall notify Technology Services and Police Services. Messages sent via e-mail using the District's network or server(s) are a limited forum, similar to the school newspaper, and therefore, the District, the principal, or the classroom teacher may restrict student speech for valid educational reasons as set forth within Education Code section 48907. The District will not restrict a student's speech on the basis of a disagreement with the opinions a student expresses. Employees' use of email is governed by BP 4040.1 (a) EMPLOYEE USE OF EMAIL.
- Network use that disrupts the use of the network by others is unacceptable.
- Users are required to obey the copyright laws and all other applicable laws and regulations.
- Users shall exhibit exemplary behavior on the network or while using District electronic equipment and while using the wireless capability features of any

- personal electronic device while representing the District, while on District property or during District sponsored events while representing the District.
- As necessary, the District will make determinations on whether specific uses of the network or personal electronic devices while on District property or during District sponsored events are consistent with the acceptable use practice.

9. If a student commits vandalism which constitutes a violation of Education Code section 48900 (f), the student may be subject to disciplinary action for such vandalism in accordance with existing policies and the Education Code. Vandalism shall result in the cancellation of privileges under this policy. Vandalism is defined as the willful or malicious destruction of public property. Vandalism includes, but is not limited to, the creation or uploading of computer viruses and/or harming or destroying data of another user or network, or a compromise (a breach, unauthorized access, suspected unauthorized changes, deletions, additions, or viewing) to one or more of the District's Enterprise Data Systems (SISWeb, QSS, Email, Network Accounts; any system used district or school wide). Students may also be subject to disciplinary action under other relevant grounds for violation of this policy and other applicable policies.

10. Theft or Damage to Electronic Files or Data Bases (Computer System Tampering or Hacking)

In the event that the system has been compromised or believed to have been compromised the following guidelines have been established.

Any employee, upon learning that a compromise (a breach, unauthorized access, suspected unauthorized changes, deletions, additions, or viewing) to one or more of the District's Enterprise Data Systems (SISWeb, QSS, Email, Network Accounts; Any system used district or school wide) has potentially occurred, shall notify immediately, their supervisor who shall notify the appropriate Associate Superintendent and the Director of Technology Services to initiate a prompt investigation.

The appropriate District Administrator, Director of Elementary, Secondary Education, or Adult Education shall notify the following departments of the potential compromise and investigation:

- Superintendent (Who will inform the Board of Education or designate a person who will inform the Board of Education of the investigation)
- Principal or Department Manager
- Police Services
- Technology Services
- Communications
- Student Services (student involvement suspected/confirmed)
- Human Resources (staff involvement suspected/confirmed)
- Risk Management

School or department administration will contact the Director of Technology Services and the Chief of Police as the first step when initiating an investigation. Alleged offenders should not be interviewed or notified of suspicions at this stage unless agreed to by the Director of Technology Services and the Chief of Police. In collaboration with Police Services and Technology Services, the school or department will utilize all available resources including but not limited to Human Resources and the Office of Student Services and appropriate Law Enforcement agencies as deemed necessary.

Prior to issuing any discipline or recommending disciplinary action to any alleged student offenders a review of findings will be provided to Human Resources and/or the Office of Student Services. Coordination as appropriate with Law Enforcement shall include, but not be limited to Sacramento County Sheriff's Department, High Tech Crime Unit, with guidance from Sacramento County District Attorney's staff, who will conduct their own investigation as appropriate. The District will provide them with complete access to all information the school or Technology Services may have obtained subject to any confidentiality requirements related to student or employee records.

School or department administration, working with Technology Services will keep time and cost accounting logs documenting the staff hours for the investigation for possible restitution and evidence for any disciplinary hearing. The investigation will be treated as a high priority by Technology Services and Police Services, recognizing that time is of the essence.

School or department administration will coordinate an incident review meeting that involves Police Services, Technology Services, identified department management and the appropriate Associate Superintendent. Upon reviewing the results of the investigation, a decision about disciplinary action for the alleged student offenders will be recommended to the Superintendent.

School or department administration in consultation with the Office of Student Services will conference with alleged offender(s) in order to inform them of the reason for disciplinary action and allow an opportunity to present their version and evidence in defense of the alleged violations prior to the school issuing a suspension and notifying the parent or guardian of the disciplinary action.

Employees who violate this policy may be disciplined in accordance with the provision of District policies and the provision of appropriate employee collective bargaining agreements. When the alleged offender is an employee of the District, she/he must be made aware of, and afforded their right to representation.

All media requests shall be coordinated through the Communications Department. School Administration shall immediately advise the Communications Department if the media arrives at the school campus.

Web Page Design

Access to the INTERNET through the Elk Grove Unified School District and creation of a Web Page using the District's network or server and as part of the educational program is a limited forum, similar to the school newspaper, and the District will exercise its rights within the law to regulate speech within that forum. Therefore, the district, the principal, or the classroom teacher may restrict student speech pursuant to Education Code section 48907 if the speech is obscene, libelous, slanderous, or likely to incite students and create a clear and present danger to the operation of the schools, or otherwise interferes with the educational mission of the district. The district will not restrict a student's speech on the basis of a disagreement with the opinions a student expresses. Web Pages are defined as actual HTML pages, blog pages, portal entries or other representation/depiction on the World Wide Web.

The following shall be adhered to when staff design Web Pages for display, or utilize web pages on the INTERNET in connection with their work, or post or allow the posting, of student web pages or student work:

1. Web pages must support course objectives and be educationally informative.
2. Photos of students along with their first name only may be posted to an Elk Grove Unified School District web page to support course objectives or if educationally informative if:
 - The full names or last names of the students are not posted along or with the photo and
 - The student does not have an opt-out form on file requesting that their photo not appear on web pages.
 - The web page is approved by a teacher and/or administrator.
3. In order to post photos of students along with their first and last name, parent/guardian written permission must be obtained before a student's photograph is placed on an Elk Grove Unified School District web page. The page must still be approved by a teacher and/or administrator. The only exception to this rule is the posting of student photos into an EGUSD administrative system such as the student information system (SISWeb) or the library system. Because these are considered closed, logon only systems, student photos are allowed without parental approval.
4. Parent/guardian written permission must be obtained and teacher/administrator approval before a video is posted containing students and before a video conferencing session involving students begins.

5. Electronic Student Newspapers are required to follow these same requirements.
6. Students' last names, mailing addresses, and/or phone numbers shall not be posted in any public web space or private web space unless parent/guardian written permission is obtained before the information is posted. One exception to this is in the case of Technology Services and Superintendent's Cabinet approved Application Service Providers (ASP's). Student data may be loaded or transferred to an ASP system in order to meet district or school needs if the application/system, the ASP vendor, and associated security measures have been approved by the Superintendent's Cabinet and Technology Services.

The following shall be adhered to regarding Student Web Pages:

1. Students will receive instruction on the design of Web Pages.
2. A teacher or administrator may authorize the posting of Student Web Pages (and/or student work) that support course objectives or are educationally informative on an Elk Grove Unified School District web page if student and parent/guardian written permission is obtained before posting. Additionally, any student work that contains photos or videos of other students must comply with requirements of this regulation prior to posting.

Policy
Adopted: July 5, 1994
Revised: April 6, 1998
June 17, 2002
December 7, 2005
January 4, 2006
April 30, 2008
September 19, 2008
January 21, 2009

ELK GROVE UNIFIED SCHOOL DISTRICT
Elk Grove, California



EGUSD Use of Technology in Instruction Application for Educational Use of the Internet

Elk Grove Unified School District provides limited access to the Internet, which includes local, national and international sources of information via its local network. Every EGUSD user has the responsibility to respect and protect the rights of every other user in our community and on the Internet. Student account holders are expected to act in a responsible, ethical and legal manner on the Internet. Students are taught network etiquette and are expected to follow it. To become a user, students and their parents must complete this form and return it to their school.

Students using these systems are subject to having all activities, including e-mail, monitored by system or security personnel. EGUSD has taken all reasonable steps to ensure the Internet is used only for purposes consistent with the curriculum. The district or school cannot prevent the availability of material elsewhere on the Internet that may be deemed harmful or intended for adults, especially to someone determined to find it. Information obtained via the Internet is at the user's risk. Using the network is a privilege, not a right, and a student's privilege may be revoked at any time for unacceptable conduct. Please read the information online at http://www.egusd.net/discover_EGUSD/pdfs/AR_6162_7.pdf

Your signature below gives your permission for your student to use the district's network and Internet access, and also confirms your understanding of the rules associated with the network. You also understand that any user who breaches these guidelines may lose all privileges on the network and/or be subject to appropriate disciplinary or legal actions.

(please print)

Student's Name: _____

Date: _____

Home Address: _____

Student Signature: _____

Student Identification #: _____

Parent/Guardian's Signature: _____

Please return this form to your child's school office.