Electronic Resource Guidelines

1. **PERSONAL RESPONSIBILITY** I accept personal responsibility for reporting any misuse of the network to the site administrator. Misuse can come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described below. Physical damage is defined as any malicious destruction to computing equipment, which is recognized as School or Private Property, as noted in Education Code section 48900 and presented to Parents in the "Parent Rights and Responsibilities" Document and the associated signed Acknowledgement Form. I understand that all rules of conduct described in the School Handbook apply when using the network. Use of the network in violation of Education Code sections 48900, 48900.2, 48900.3, or 48900.4 will lead to disciplinary action including suspension, expulsion, or prosecution when appropriate.

2. **DISTRICT AND SCHOOL WEB SITES** Links placed on district and school web sites shall conform to the following:
   a. The District or school's Web page is a District publication. It is, and is intended to be a closed forum.
   b. The District or school's Web page was created for the express purpose of disseminating educational and administrative information. The District maintains full authority to regulate and limit access and content.
   c. The purpose of the Web page is to enhance the educational process and promote the educational mission of the District.
   d. The District reserves the Web page for legitimate educational purposes only.
   e. As the Web page is a closed forum, the District reserves the right to regulate the content of the items posted in keeping with its educational purpose.
   f. Students and teachers and other unauthorized District employees may not post or alter items on the Web page. The District does not authorize access for teachers and students to post or alter items. Likewise, the general public may not post items on the Web page.
   g. Items pertaining to courses, school or District functions, or related activities may be submitted to the designated administrator who will determine whether and in what format to include such items on the Web Page, according to adopted standards.

3. **PRIVILEGES** The use of the information system is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. Each person who receives an account will participate in an orientation or training course with a faculty member as to proper behavior and use of the network. The site administrator will decide what is appropriate use and his/her decision is final. The site administrator may close an account at any time when deemed necessary. The administration of the Etiwanda School District may deny, revoke, or suspend specific user accounts.

4. **NETWORK ETIQUETTE AND PRIVACY** You are expected to abide by acceptable rules of network etiquette. These rules include, but are not limited to, the following:
   a. **BE POLITE** Never send, or encourage others to send, abusive messages.
   b. **USE APPROPRIATE LANGUAGE** You may be alone with your computer, but what you say and do can be viewed globally. Never swear, use vulgarities, or any other inappropriate language. Illegal activities of any kind are strictly forbidden, and are subject to disciplinary action including suspension and/or expulsion.
   c. **PRIVACY** Do not reveal your home address or phone number or the addresses or phone numbers of students or colleagues. Do not reveal other personal information, such as your age, marital status, financial information, your work address or telephone number, nor your parent's work address or telephone number.
   d. **ELECTRONIC MAIL** When using the district's technology resources, users do not have an expectation of privacy in anything they create, store, delete, send or receive on the district's technology resources. The use of the technology resources shall constitute express consent to being monitored. This consent shall authorize the district's representative(s) to monitor, without prior notification or consent, all technology resource use including, but not limited to, internet use, e-mails, audio or visual material, computer transmissions, stored information and deleted information or files. Messages relating to or in support of illegal activities must be reported to the authorities. User is responsible for any information sent through the user's email account. Protection of one's password is vital. If a password is shared for maintenance or other purpose, immediate change is recommended. (Etiwanda School District Employees see "Email Addendum" for further guidelines).
   e. **DISRUPTIONS** Do not use the network in any way that would disrupt use of the network by others. Do not read other users' mail or files or attempt to interfere with other users' ability to send or receive electronic mail. Do not attempt to read, delete, copy, modify, or forge other users' mail.
   f. **MESSAGES / BULLETIN BOARDS** Never respond to messages or bulletin board items that are sexually suggestive, obscene, belligerent, threatening, or make you feel uncomfortable.
   g. **INFORMATION** Do not place unlawful information on any network system.
   h. **OTHER CONSIDERATIONS:**
      - **Do** be brief. Few people will bother to read a long message.
      - **Do** minimize spelling errors and make sure your message is easy to understand and read.
      - **Do** use accurate and descriptive titles for your messages. Tell people what it is about before they read it.
      - **Do** get the most appropriate audience for your message, not the widest.
      - **Do** remember that humor and satire are very often misinterpreted.
      - **Do** remember that if you post to multiple groups, specify all groups in a single message.
      - **Do** cite references for any facts you present.
      - **Do** forgive the spelling and grammar errors of others.
      - **Do** keep signatures brief.
      - **Do** remember that all network users are human beings. Don't "attack" correspondents; persuade them with facts.
      - **Do** post only to groups you know.

5. **SERVICES** The Etiwanda School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages including loss of data as a result of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the information system is at your own risk. The District specifically disclaims any responsibility for the accuracy of information obtained through its electronic information services.

6. **SECURITY** Security on any computer system is a high priority because there are so many users. If you identify a security problem, notify the teacher or site administrator at once. Never demonstrate the problem to other users. Never use another individual's account without written permission from that person. All use of the system must be under your own account. Any user identified as a security risk will be denied access to the information system.

7. **VANDALISM** Vandalism is defined as any malicious attempt to harm, disrupt or destroy computer resources. This includes, but is not limited to:
   a. The introduction or creation of computer viruses, worms, trojans, malware or spyware.
   b. Any attempt to harm the District network, equipment, materials, or data.
   c. Tampering or destroying the data of another user, agency or network that is connected to the district infrastructure.

   Any vandalism will result in the loss of computer privileges, disciplinary action including suspension, expulsion and/or legal action.

8. **UPDATING** The information service may occasionally require new registration and account information from you to continue the service. You must notify the information system of any changes in your account information.

9. **DISCLAIMER** The District makes no warranties of any kind, whether expressed or implied, for its technology services. The District is not responsible for any damages that occur from the use of the District's computer system, including loss of data or service interruption. Use of information obtained via electronic mail is at the user's own risk. The District is not responsible for the accuracy of information obtained through electronic information resources.

   The district reserves the right to change the terms and conditions of the *Acceptable Use Rules and Regulations*. Any changes will be posted on the District network. Continued access of the technology once changes to any policy have been made will constitute the user's acceptance of the amended terms.

   The District reserves the right to delete, without notice, from email messages and school, class, or student Web pages, any material violating the *Acceptable Use Rules and Regulations*. The District is not responsible for monitoring the content of any message or Web page and failure to detect or delete such material shall not constitute sponsorship of such material or waiver of the right to delete it in the future.

10. **MOBILE DEVICE GUIDELINES** The purpose of the use of technology in a K-12 educational organization is to further the academic performance of our students and to equip the students, staff and administrators in performing the business and educational functions of the organization. Mobile Computing Devices are products that can help accomplish this objective.

    The purchase and use of a Mobile Computing Device should be based on the following:
    a. The device is required to support a specific instructional and/or administrative requirement that can best be accomplished through this device;
    b. Broadband, and personal wireless content service providers and associated contracts will be approved by the Superintendent and Cabinet;
    c. Any organizationally purchased Mobile Computing Device must meet the Mobile Computing Device Standards that will be published annually by the Technology Department.

    The definition of Mobile Computing Devices shall be: eReaders (Nook, Kindle and other tablet-style devices), Laptops, Netbooks, iPods, iPads and future devices as approved by the Superintendent or designee. In using Mobile Computing Devices all employees and students must abide by the district's Employee Use of Technology and Student Use of Technology policies.

    Organizationally purchased Mobile Computing Devices are the property of the district. All organizationally purchased Mobile Computing Devices shall be tagged in accordance with inventory policies and procedures. Employees and students shall also follow district policy regarding use of organizationally purchased equipment off premises.

    Annually the Technology Department shall set a standard for Mobile Computing Device purchases. These minimum requirements shall be posted on the district's web site for employee access at the start of each fiscal year. The Purchasing/Contracts Department shall purchase in accordance to these standards and follow all applicable Purchasing/Contracts policies and procedures.

    Mobile Computing Devices and any associated applications (apps) purchased by the organization will be approved by the department/school site making the purchase. The organization's purchase of the digital devices and apps will be through the regular requisition process. The requisition will clearly state a justification for the device or apps. Once the requisition has cleared the approval path, the designated volume purchaser(s) shall obtain the apps and notify the end user once redemption codes are issued. The downloading of organizationally purchased apps to personally owned devices shall be prohibited as it may constitute a gift of public funds.

Security

Organizationally purchased Mobile Computing Devices will be subjected to the same Acceptable Use Policies and network security policies that are in place for other networkable devices. As security enhancements are added or strengthened in the device's OS, then those features will be analyzed by technical staff and implemented accordingly. Organizationally purchased Mobile Computing Devices will be initially configured and managed by authorized staff. Employees are discouraged from loading personal data, and strictly prohibited from loading sensitive or confidential data onto the organizationally purchased mobile device unless instructed otherwise in writing. Personal Mobile Computing Devices used for business purposes will be subject to the same policies as organizationally purchased Mobile Computing Devices stated above.

Device Standards: Smartphones/PDAs by Carrier for Southern California Area

Authorized employees requiring smart phone access to e-mail, calendar, and contact lists must have a phone which natively supports Microsoft Exchange accounts.

The following is a list of acceptable devices:

IPhones:	IOS 4.0 or greater
Windows Phones:	WINDOWS MOBILE 6.0 or greater
WINDOWS Phone:	7 or greater
ANDROID Phones:	OS 2.1 or greater

IMPORTANT: BLACKBERRY (RIM Technology) devices that do not natively support Microsoft Exchange without BIS integration are not supported by the Superintendent's network infrastructure and are not eligible for stipend reimbursements.

11. MOBILE DEVICE SECURITY and USAGE OVERVIEW This section describes the security guidelines for mobile devices. Like desktop computers, mobile devices (such as cell phones, PDAs, and laptop computers) must be appropriately secured to prevent sensitive data from being lost or compromised, reduce the risk of spreading viruses, and mitigate other forms of abuse of the Etiwanda School District's computing infrastructure.

In order to secure information stored in a mobile device, employees should adhere to some general "best practices" when using mobile devices.

Additional measures may be possible and appropriate for securing your specific device.
For detailed information on Mobile Device Security and Usage Guidelines, see "Guidelines for Mobile Computing Devices Supplement."

User Responsibilities and Procedures

PASSWORD-PROTECT YOUR MOBILE DEVICE Physical security is a major concern for mobile devices, which tend to be small and easily lost or misplaced. If your mobile device is lost or stolen, a device password may be all that stands in the way of someone reading your email and other sensitive data.

Choose a strong password. The security of your system is only as strong as the password you select to protect it.

It may be difficult to type especially complex passwords on the small keypad of some devices, but it is important that you try to choose a strong, effective password that is not easily guessed. Use the guidelines available at http://intranet.etiwanda.org/docs/passwordsec.htm.

Use antivirus software: Mobile devices can be just as susceptible to viruses as desktop computers. This is new terrain for hackers but, industry analysts expect viruses, Trojans, spam, and all manner of scams to grow as the mobile device market grows.

PROMPTLY REPORT A LOST OR STOLEN DEVICE If you are receiving district email on your mobile device, you must report the event immediately to the Technology Department by phone or email (postmaster@etiwanda.org). In some cases, a device can be remotely deactivated thus preventing email or other sensitive data from being exposed. Understand what options are available to you and exercise them promptly when necessary. Additionally, consider documenting the serial number of and/or engraving your device.

VERIFY ENCRYPTION MECHANISMS Your accounts and passwords should never travel unencrypted over a wireless network. Wireless network traffic can be easily obtained. Therefore, any sensitive data, especially login information, should always be encrypted.
Sensitive documents, if stored on the device, should be encrypted if possible (keeping in mind that some devices encrypt stored documents by default).

DISABLE OPTIONS AND APPLICATIONS THAT YOU DON'T USE Reduce security risk by limiting your device to only necessary applications and services. You won't need to manage security updates for applications you don't use and you may even conserve device resources like battery life. Bluetooth and IR are two examples of services that can open your device to unwelcome access if improperly configured.

REGULARLY BACK UP DATA Be sure to have a back-up copy of any necessary data in case your mobile device is lost or damaged. Consider using multiple backup mechanisms and if you travel, have a portable backup device that you can take with you.

FOLLOW-UP SAFE DISPOSAL PRACTICES When you are ready to dispose of your device, be sure to remove all sensitive information first.

12. CYBER-BULLYING

Cyber Bullying Definitions:

Bullying shall mean unwelcome verbal, written or physical conduct directed at a student by another student that has the effect of

a. Physically, emotionally or mentally harming a student;
b. Damaging, extorting or taking a student's personal property;
c. Placing a student in reasonable fear of physical, emotional or mental harm;
d. Placing a student in reasonable fear of damage to or loss of personal property; or
e. Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.

Cyber-bullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member employing any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, text messages, digital pictures or images, or website postings (including blogs) which has the effect of:

a. Physically, emotionally or mentally harming a student;
b. Placing a student in reasonable fear of physical, emotional or mental harm;
c. Placing a student in reasonable fear of damage to or loss of personal property; or
d. Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.

All forms of bullying are unacceptable and, to the extent that such actions are disruptive of the educational process, offenders shall be subject to appropriate staff intervention, which may result in administrative discipline.

The term "bullying" and "cyber-bullying" shall not be interpreted to infringe upon a student's right to engage in legally protected speech or conduct.

Delegation of Responsibility:

a. Each staff member shall be responsible to maintain an educational environment free of bullying and cyber-bullying.
b. Each student shall be responsible to respect the rights of his/her fellow students and to ensure an atmosphere free from all forms of bullying and cyber-bullying.
c. Students shall be encouraged to report bullying or cyber-bullying complaints to an appropriate staff member.
d. Any staff member who receives a bullying or cyber-bullying complaint shall gather information or seek administrative assistance to determine if bullying or cyber-bullying has occurred. If the behavior is found to meet the definition of bullying or cyber-bullying, the school administration must complete the appropriate written documentation (see Bullying, Cyber-Bullying, Harassment or Intimidation Reporting Form).
e. The school administration or his/her designee will inform the parents or guardians of the victim and also the parents or guardians of the accused.

Complaint Procedure:

a. Student shall report a complaint of bullying or cyber-bullying, orally or in writing, to a staff member. If a parent initiates the complaint, the appropriate staff member will follow-up with the student.
b. The staff member will either gather the information or seek administrative assistance to determine if the alleged bullying or cyber-bullying conduct occurred.
c. After the information has been gathered, the school administration shall be notified of the complaint. The school administration will determine the need for further investigation or the appropriate intervention, which may result in administrative discipline to ensure that the conduct ceases. If the behavior is found to meet the definition of bullying or cyber-bullying, the school administration must complete the appropriate written documentation.

***Students* - A violation of this Policy shall subject the offending student to appropriate disciplinary action, consistent with the student discipline code, which may include suspension, expulsion or referral to the appropriate authorities.**

***Employees* - Actions in violation of these policies are outside the scope of employment.**