

POLICY

Dr. Lena Edwards Academic Charter School

Safe & Responsible Internet Use Plan

The school has technology protection measures for all computers in the school that block and/or filter visual depictions that are obscene, contain child pornography and are harmful to minors as defined in the Children's Internet Protection Act.

The school certifies that the school is in compliance with the Children's Internet Protection Act and Acceptable Use Policy. Compliance measures contained within this plan address the following:

Access by Minors to Inappropriate Matter on the Internet

Users will not use the school electronic network to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination toward other people (hate literature).

For students, special exception may be made for hate literature if the purpose of such access is to conduct research, AND access is approved by both the teacher and the parent. School employees may access the above material only in the context of legitimate research. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by the school. Students should immediately notify teachers. Teachers and staff should immediately notify building administration. Building administration should immediately notify technology coordinator. This will protect users against an allegation that they have intentionally violated the Acceptable Use Policy. The fact that the filtering software has not protected against access to certain material shall not create the presumption that such material is appropriate for users to access. The fact that the filtering software has protected access to certain material shall not create the presumption that the material is inappropriate for users to access. The Board will provide student access to Internet resources only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain.

Safety and Security of Minors when using Electronic Mail, Chat Rooms, and other Forms of Direct Electronic Communications and Unauthorized Disclosures

Student users will not post or share contact information about themselves or other people. Personal contact information includes the student's name together with other information that would allow an individual to locate the student, including, but not limited to, parent's name, home address or location, work address or location, or phone number.

Elementary school students will not disclose their full name or any other personal contact information for any purpose. Students will not disclose names, personal contact information, or any other private or personal information about other students under any circumstances. Students will not forward a message that was sent to them privately without permission of the person who sent them the message. Students will not agree to meet someone they have met online. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable. Students should not delete such messages until instructed to do so by a staff member.

Unauthorized Access, Including "Hacking" and other Unlawful Activities by Minors Online

Security on any computer network is a high priority, especially when the network involves many users. If a user feels that he/she can identify a security problem on the computer network, the user must notify a Network

Administrator or building level administrator. The user should not inform individuals other than the network administrators or building administrators of a security problem. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use this account. Under no conditions should a user provide his/her password to another person. Passwords to the network should not be easily guessable by others, nor should they be words that could be found in a dictionary. Attempts to "log on" to the network using either another user's account or as a network administrator could result in termination of the account. Users should immediately notify a network administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their accounts. Any user identified as a security risk will have limitations placed on usage of the network or may be terminated as a user and be subject to other disciplinary action. Users will not attempt to gain unauthorized access to the school system, or go beyond their

authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing". Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal. Users will not use the school system to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.

Technology Protection Measure (Software Filtering)

The school has selected a technology protection measure (software filtering) for use with the school Internet system. The filtering software will always be configured to protect against access material that is obscene, child pornography and material that is harmful to minors, as defined by the Children's Internet Protection Act.

The school may, from time to time, reconfigure the filtering software to best meet the educational needs of the school and address the safety needs of the students. The technology coordinator will conduct an annual analysis of the effectiveness of the selected filter. The Lead Person will make recommendations to the Board regarding the selection and configuration of the filter in the event that changes to the filter are necessary. The filter may not be disabled at any time that students may be using the Internet system, if such disabling will cease to protect against access to materials that are prohibited under the

Children's Internet Protection Act. The filter may be disabled during non-student use time for system administrative purposes. Filtering software has been found to inappropriately block access to appropriate material. To ensure that the implementation of the technology protection measure is accomplished in a manner that retains school control over decision making regarding the appropriateness of material for students, does not unduly restrict the educational use of the school Internet system by teachers and students, and ensures the protection students' constitutional right to access to information and ideas, authority will be granted to selected educators to temporarily or permanently unblock access to sites blocked by the filter.

Authority to temporarily unblock access will be granted to building administrators and or his/her designees, and any teacher who regularly uses the Internet for instructional purposes who request permission to have such authority. Individuals granted authority to temporarily unblock sites must meet standards for technical proficiency that are deemed necessary to ensure the security of the system. The Technology Coordinator shall determine such

standards. To temporarily unblock a site, the authorized individual must review the content of the site, outside of the presence of any student, prior to allowing access to the site by a student. Reports of all instances of temporary unblocking will automatically be forwarded to the Technology Coordinator. If an unauthorized individual believes that the blocked site should be permanently unblocked, a recommendation will be forward to the supervisor of technology. The supervisor of technology will make a decision to permanently unblock access to the site or may delegate the decision to the school technology committee. An electronic list of all sites that have been permanently unblocked will be housed in the technology department. A request to unblock process will be established in secondary libraries to allow students to anonymously request that a blocked site be temporarily or permanently unblocked.

Notwithstanding the visual depictions defined in the Children’s Internet Protection Act and as defined in this Plan, and Policy and Regulation 2361, the Board shall determine Internet material that is inappropriate for minors. The school will post this Safe & Responsible Internet Use Plan on the school web site, with links to the Acceptable Use Policy & Regulation document, and recommended Internet safety sites for parents.

Date Adopted:

A survey will be conducted with school teachers in spring of 2013 to provide insight into their proficiency with basic technology skills, understanding of technology goals and standards, and the level of technology integration in instruction. Training will be established to meet identified needs.

The technology survey categories provided the ability to analyze the results according to the following:

- Technology Operations and Concepts
- Types of Professional Development they participated in
- Knowledge of Technology Goals and Standards
- Planning, Teaching, Learning, Assessing and Curriculum
- Social, Ethical, Legal and Human Issues