P1232 ACCEPTABLE USE OF COMPUTERS, NETWORKS, INTERNET, ELECTRONIC MAIL, TELEPHONES, AND OTHER ONLINE SERVICES – STUDENTS

BOARD POLICY:

USD 259 is committed to making advanced technology and increased access to learning opportunities available to all students. The goal of the district in providing access to students is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. The use of computers, networks, the Internet, or other online services shall be in support of education and research consistent with the district's educational objectives.

Administrative Implemental Procedures:

1. Student Responsibilities**.** Regardless of any "technology protection measure" implemented by the District as may be required by the Children's Internet Protection Act**,** students are responsible for good behavior on computers, networks, the Internet, or other online services just as they are in a classroom or a school hallway. General school rules for behavior and communications apply. Network storage areas will be treated like school lockers. Network administrators, teachers, and other appropriate district staff may review student files and student communications from time to time to prevent misuse and to ensure students are using the system responsibly and in compliance with laws and district policies. Communications on the network are often public in nature; students should not expect that files stored on district servers will be private.
2. Permission. Students must have permission from and be under the supervision of school district professional staff before utilizing district-provided computers, networks, the Internet, or other online services. Permission is not transferable from one student to another and may not be shared. Students shall not be allowed to utilize electronic communications unless a signed Student Access Contract is on file. To remain eligible as users, students' use must be consistent with the educational objectives of the district. Access is a privilege, not a right, and inappropriate use will result in, among other disciplinary measures, the cancellation of those privileges. Students will display school-appropriate conduct when using the computer equipment or network and shall maintain an environment conducive to learning.
3. Violations. Administrators, teachers, and other appropriate district employees will decide what is inappropriate use. Violating this policy may result in:
   a. Restriction or loss of network access; and/or
   b. Disciplinary or legal action including, but not limited to, suspension or expulsion from school and/or criminal prosecution under appropriate local, state, and federal laws; and
   c. Assessment of the cost of damages to hardware/software.

4. Inappropriate Use. The following uses of school-provided computers, networks, the Internet, or other online services are not permitted on the part of USD 259 students:
    a. Accessing, uploading, downloading, or distributing pornographic, obscene, or sexually explicit material;
    b. Transmitting obscene, abusive, sexually explicit, or threatening language;
    c. Violating any local, state, or federal statute;
    d. Accessing another individual's materials, information, or files without permission.
    e. Violating copyright or otherwise using the intellectual property of another individual or organization without permission;
    f. Using others' passwords;
    g. Vandalizing, defined as any unauthorized access and/or malicious attempt to damage computer hardware/software or networks or destroying the data of another user, including creating, uploading, or intentionally introducing viruses;
    h. Intentionally wasting limited resources;
    i. Using the network for commercial purposes;
    j. Bullying, harassing, insulting, or attacking others;
    k. Using, disclosing, or disseminating personal information online such as full name, home address, phone number, etc., except with approval by certified or administrative district staff;
    l. Using e-mail lists from the district's Internet site, network, or servers to create mailing lists for non-school purposes;
    m. Gaining unauthorized access to resources or entities;
    n. Invading the privacy of individuals;
    o. Improperly altering the setup of computers (e.g., desktops, icons, wallpapers, screensavers, installed software) as determined by the network administrator;
    p. Using software that has not been assigned or approved by staff;
    q. Failing to follow a district policy while using computers or failing to follow any other policies or guidelines established by district administration, teachers, or other appropriate district staff; and
    r. Seeking to gain or gaining unauthorized access to information resources or other computing devices.
5. Security Risk. Any student identified as a security risk or having a history of problems with other computer systems may be denied access.
6. Disclaimer. The district makes no warranties of any kind, whether express or implied, for the access it is providing. The district will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, 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. The district denies any responsibility for the accuracy or quality of information, or for any commercial transactions conducted through its system.
7. Statements of Personal Belief. Any statement of personal belief found on computers, networks, the Internet, other online services, telephones, or other telecommunication system is implicitly understood to be representative of the author's individual point of view, and not

that of USD 259, its employees, or the participating school. No representations to the contrary shall be published without written approval from the district. Principals or district administrators may review all content in any Internet or online accounts paid for, in whole or in part, by the district or any school, without notice of any kind.

8. Student Access Contract. Prior to use of school computers or networks, (e.g. the Internet or other online services), each student shall submit a signed Student Access Contract for filing in the school office. Prior to use of computers at any other district facility, each student shall also submit a signed Student Access Contract for filing with the main office of the facility at which these computers are located. If a student is under the age of 18, a parent/guardian shall also sign the contract(s). New Student Access Contracts must be signed and submitted each school year. BOE Policy 1232 applies to all students regardless of whether they have submitted a signed Student Access Contract. If a student does not have a current Student Access Contract on file as required above, access to computer services and accounts is prohibited.
9. District Technology Plan. The Administrative Implemental Procedures contained in this policy shall be consistent with the District Technology Plan adopted by the Board of Education.

Approved as to form and content by Board attorney.

Administrative Responsibility: Information Services and Technology
Latest Revision Date: January 2013 P1232
Previous Revision Date: January 2002