P1231 ACCEPTABLE USE OF COMPUTERS, NETWORKS, INTERNET, ELECTRONIC MAIL, AND OTHER ONLINE SERVICES - EMPLOYEES

BOARD POLICY:

The district will provide administrators, teachers, and other employees access to computers, networks, Internet, electronic mail (e-mail), and employee data systems through the district's internal and external Portal accounts. The purpose of this access is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. The use of computers, networks, the Internet, e-mail, and other on-line services shall be in support of education and research consistent with the educational objectives of the district.

Administrative Implemental Procedures:

1. Services. The school district encourages employees to learn to use computers, networks, Internet, e-mail, and other online services and apply these tools in appropriate ways to the performance of tasks associated with their positions and assignments.

2. Multiple Computers. No district employee is allowed to have more than one (1) computer. Employees are allowed either one (1) desktop computer or one (1) laptop computer, but not both. Any and all exceptions must be requested in writing and submitted to the USD 259 Chief Information Officer (CIO) for review.

3. Appropriate Use. Employees shall communicate with telecommunication tools in a professional manner consistent with state laws and district policies governing the behavior of school employees and with federal laws governing copyright. For compliance with electronic discovery rules, employees are required to use district e-mail, rather than personal e-mail accounts, to conduct district business. E-mail and telecommunications shall not be improperly utilized to disclose confidential information about district employees or to disclose information from student education records in violation of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, as amended, and its interpretive regulations, 34 C.F.R. § 99.1, et seq. This shall not apply to the student information system program or other district administrative software that is to be used by authorized employees in a manner that complies with FERPA and its interpretive regulations. (See P5501 - Privacy of Student Records and the district guidelines for FERPA.)

    a. It is the responsibility of all District employees and/or persons with access to district data (including contractors and volunteers) to maintain the highest level of security to prevent data stored on portable devices from being accessed by unauthorized individuals. Portable devices include, but are not limited to, laptop computers, jump drives, and external hard drives.

4. Public Communication. Communication over networks should not be considered to be private. Messages may be diverted accidentally to another destination. The district network administrator(s) from time to time may review directories, files, or e-mail to ascertain compliance with network guidelines for acceptable use and/or appropriate personnel action. In addition, e-mail and other electronic files may be reviewed for other purposes, such as litigation and open records requests. The network administrator(s) may delete files that are not kept to a manageable storage level or are deemed inappropriate.

5. Student Access. Regardless of any "technology protection measure" implemented by the District as may be required by the Children's Internet Protection Act, teachers, administrators, and others who make decisions regarding student access to the Internet shall, in making such decisions, at all times consider the district's stated educational mission and the student acceptable use policy. To the extent possible, students' use of the Internet shall be structured in ways that point students to those resources that have been evaluated prior to use. District professional staff shall supervise students utilizing district-provided Internet access. Students shall not be allowed to utilize electronic communications unless a signed consent is on file. A family's right to decide whether or not to sign the Student Access Contract for their student shall be supported and respected. Permission is not transferable from one student to another and may not be shared.
6. Violations. Employees who violate this policy will be subject to appropriate disciplinary action, up to and including termination.
7. Inappropriate Use. The following uses of school-provided access to computers, networks, Internet, e-mail, and other online services are not permitted on the part of district employees:
    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 employee's materials, information, or files without permission from the employee or the appropriate network administrator or principal;
    e. Violating copyright or otherwise using the intellectual property of another individual or organization without permission, specifically including, but not limited to the unlawful downloading of music, movies, computer software, or pictures;
    f. Using others' passwords and allowing students or third parties who are not employed by the district to use staff members' passwords;
    g. Vandalizing, which is 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, including, but not limited to, storage of excessive amounts of personal e-mails, movies, music, and picture files on district computers or servers;
    i. Using the district's network or computers for commercial purposes, including, but not limited to, selling items, and maintenance of a personal or business website or e-mail accounts;
    j. Harassing, bullying, insulting, or attacking others;
    k. Accessing or transmitting e-mail or other electronic files containing inappropriate and/or offensive material that is aimed at members of any protected class (examples would include jokes targeted at person(s) based upon gender, race, ethnicity, disability, etc.);
    l. Using e-mail lists from the district's Internet site, network, or servers to create mailing lists for non-district 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, or installed software) as determined by the network administrator;

p. Failing to follow district policies while using computers or failing to follow any other policies or guidelines established by district administration or the user's supervisor and failure to follow instructions of supervisors; and
q. Seeking to gain or gaining unauthorized access to information resources or other computing devices;
r. Using district resources to create or access personal e-mail accounts to conduct district business or to engage in conduct that would violate any district policy.
s. The use of or participation in social media networks for personal use while on district time or on district equipment. For more information, see the USD 259 Guidelines for the Use of Social Media.

8. Security. Users are responsible for maintaining a safe, secure environment:
   a. Users will keep passwords secure; and
   b. Users will change passwords when directed by the network administrator.

9. Security Risk. Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

10. Copyright law shall be respected for all Internet and online services. (See P6400 - *Copyrights*.)

11. Disclaimer. The district makes no warranties of any kind, whether express or implied, for the access it is providing, nor will it be responsible for any damages suffered. 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. The district denies any responsibility for the accuracy or quality of information obtained through its system. The district is not liable for any commercial transactions conducted through its system.

12. Statements of Personal Belief. Any statement of personal belief found on computers, networks, the Internet, e-mail, other on-line services, or any other telecommunication system shall be implicitly understood to be representative of the author's individual point of view, and not that of USD 259, its administrators, teachers, staff, or the participating school. No representations to the contrary shall be published without written approval from the designated district-level administrator(s). Principals, district-level administrators, or their designees may review all content in any Internet or on-line accounts paid for, in whole or in part, by the district or any school, without notice of any kind.

13. Employee Access Contract and Annual Review.
   a) Prior to use of district computers, networks, the Internet, electronic mail, and other on-line services, the employee desiring to use such services shall submit a signed Employee Access Contract to the Human Resources office for filing. An Employee Access Contract must be on file in order for the employee to have access to the above services, including an Outlook account.
   b) Any employee who declines to sign an Employee Access Contract shall be denied access to the above services. In this event, the employee shall initial the Employee Access Contract to acknowledge awareness of Policy 1231. The initialed Employee Access Contract shall be submitted to the Human Resources office for filing. Thereafter, every employee must sign the employee access contract annually.
   c) Human Resources shall maintain a current list of employees who have signed Employee

Access Contracts and make it available to all principals, district office administrators, and their designees.

d) Each year, employees will be referred to the policy by Human Resources for review and electronic signature.
e) Policy 1231 applies to all employees regardless of whether or not they sign or initial an Employee Access Contract and/or attend annual review meetings related to this policy.
f) All employees who are assigned laptop computers will be required to complete the Staff Laptop Checkout form.

14. 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.

14. E-mail Publications. E-mail publications are E-mail messages addressed to multiple recipients and intended for a general audience (example – ZALLPRINCIPALS) as opposed to a specific group. Such e-mail publications are prohibited, unless authorized by the principal of the school or other appropriate supervisor (if not supervised by a school principal) that originates the message. (See P1232 Acceptable Use of Computers, Networks, Internet, Electronic Mail, and Other Online Services – Students.)

Administrative Responsibility: Human Resources
Latest Revision Date: September 2013
Previous Revision Date: August 2013 P1231

Updated administratively for alignment purposes: March 2014