DANVILLE AREA SCHOOL DISTRICT
ACCEPTABLE USE GUIDELINES FOR
INFORMATION TECHNOLOGY RESOURCES IN THE SCHOOLS

The Danville Area School District's information technology resources (and any devices brought on to DASD property), including email and Internet access, are provided for educational purposes. Adherence to the following guidelines is necessary for continued access to the district's technological resources:

Authorized users must

1. Respect and protect the privacy of others.
    - Use only assigned accounts.
    - Not view, use, or copy passwords, data, or networks to which they are not authorized. Not distribute private information about others or themselves.
2. Respect and protect the integrity, availability, and security of all electronic resources.
    - Observe all network security practices, as posted.
    - Report security risks or violations to a teacher, administrator, or technology staff member.
    - Not destroy, alter, or damage data, networks, or other resources that do not belong to them, without permission of the owner.
    - Conserve, protect, and share these resources with other authorized users.
    - Not bypass or attempt to bypass district technology protections.
    - Not install, modify, or remove software/hardware without district authorization.
3. Respect and protect the intellectual property of others.
    - Not infringe copyrights (i.e. making illegal copies of music, games, or movies).
    - Not plagiarize.
4. Respect and practice the principles of community.
    - Communicate only in ways that are kind and respectful.
    - Report threatening or discomforting materials to a teacher or administrator.
    - Not intentionally access, transmit, copy, or create material that violates the district's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
    - Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
    - Not use the resources to further other acts that violate federal/state laws and/or the district's code of conduct.
    - Not send spam, chain letters, or other mass unsolicited mailings.
    - Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.
    - Not use technology to cheat.

Authorized users may, if in accord with the policy above

1. Design and post web pages and other material from district resources.
2. Use direct communications such as online chat or instant messaging with a teacher’s or administrator’s permission.
3. Install or download software, if also in conformity with laws and licenses, and under the supervision of a teacher or technology staff member.
4. Use the resources for any educational purpose.

Signatures required on back →

Consequences for Violation. Violations of these rules will result in disciplinary action, which may include the loss of student/staff privileges to use the district's information technology resources and/or referral to law enforcement agencies.

Supervision and Monitoring. Danville Area School District administrators and their authorized employees monitor the use of information technology resources to help ensure that users are secure and in conformity with these guidelines. Administrators reserve the right to examine, use, and disclose any data found on the district's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

I ACKNOWLEDGE AND UNDERSTAND MY OBLIGATIONS:

_____ _____

Student/DASD Employee/Guest SIGNATURE Date

_____ _____

Student/DASD Employee/Guest PRINT NAME Date

_____ _____

Parent/Guardian Signature (if student) Date

PARENTS, PLEASE DISCUSS THESE RULES WITH YOUR STUDENT TO ENSURE HE OR SHE UNDERSTANDS THEM.

THESE RULES ALSO PROVIDE A GOOD FRAMEWORK FOR STUDENT/STAFF USE OF COMPUTERS AT HOME, AT LIBRARIES, OR ANYWHERE.

FOR MORE INFORMATION, SEE www.cybercrime.gov.