



Danville Staff Acceptable Use Policy

The Danville Schools offer a variety of network and Internet resources to all staff as part of the instructional process. All uses of the Danville Schools' data system must be in support of education and must be consistent with all state and district policies. This document contains the Acceptable Use Policy (AUP) for Users of the Danville Schools' data system. This document must be signed by all Users.

Network Resources and Phones

1. Each staff member will be given a Google for Education account for email, file creation, and file storage. Employees shall not access files/folders or retrieve any stored communication unless they have been given authorization to do so. Each employee is responsible for the security of his/her own password. The district will deactivate accounts upon termination of employment. It is the employee's responsibility to transfer any content he or she wants to keep to a personal account when he or she leaves the Danville Schools.
2. Staff may be assigned a mobile device (ipad, chromebook, laptop, etc.) to be used during the school year. It is the staff member's responsibility to turn in the device and charger when leaving a position, or when asked by school/district personnel. Failure to do so may result in the staff member paying a replacement cost.
3. Classroom phones and cell phones should be used for instructional purposes or emergency situations only. Personal calls and/or texts made during the school day should be during non-instructional times. Any personal long distance charges incurred from a classroom phone must be paid for by the user placing the call.

Electronic Mail and the Internet

Electronic mail accounts and Internet access will be given to all Danville Independent staff. Employees are encouraged to use email and the internet to enhance instruction, promote student learning, and provide communication with the home.

1. E-mail and Internet access is to be used for instruction, research, home communication, and school administration purposes only. Access to these resources provided by the Danville Schools is not to be used for private business or personal gain. This includes sending out "for sale" emails, shopping online during the instructional day, etc.
2. School email addresses should not be used to sign up for non-education accounts. This includes, but is not limited to: online stores (Amazon, Macy's, Bestbuy, etc.), video streaming sites (Netflix, iTunes, Hulu, etc.), other subscription type services, and utility companies.
3. Users shall not compose, send, or attach defamatory, inaccurate, abusive, profane, sexually oriented, threatening, racially offensive or illegal documents/files. This includes sending out school or district-wide emails questioning the teaching ability or actions of other staff members.
4. Users shall not visit sites that contain profane, sexually oriented, threatening, racially offensive, or other objectionable material. Users shall not try to circumvent the web filter that blocks such sites.
5. All staff and student correspondence via electronic mail should be to facilitate classroom learning. Staff should not use personal email accounts to communicate with students or parents/guardians.
6. When sending an email to a group of parents, staff should put each parent email address on the Bcc line to protect parent confidentiality.
7. Teachers, library media specialists, and other educators will select and guide students' use of computer and instructional resources at all times.
8. Users shall not transmit via email or post online a student's work or picture containing personally identifiable information without written parental consent.
9. Students should not be allowed to reveal their name or personal information or establish relationships with "strangers" on the Internet or through email unless the communication has been coordinated by a teacher and written permission is granted by the student's parent/guardian.
10. All electronic mail and Internet usage is logged and can be checked by District personnel if inappropriate conduct is suspected.
11. Users shall not use e-mail or the Internet to promote or campaign for a political candidate.
12. Students are prohibited by their AUP from playing non-educational games, or watching non-instruction videos through youtube, Netflix or other streaming sites. Staff should not encourage nor give permission to play non-educational games or stream non-instructional videos during class.

District and School Webpages

The Danville School District maintains an official district webpage as well as a webpage for each school. Each webpage has numerous subsection pages for organizations, clubs, sports, curriculum, etc. Staff members/coaches/sponsors may be given access to update various sections of the official webpage(s).

1. The use of webpages must be in support of education.
2. Users will be responsible for maintaining the content of their assigned section(s). Users will not post obscene, profane, vulgar, rude, inflammatory, threatening, or disrespectful language, materials and/or pictures.
3. Sponsors/coaches of extracurricular organizations may establish webpages. Material presented on the organization web page must relate specifically to organization activities and will include only user-produced material.
4. Users may not use the webpages for commercial purposes unless a special waiver is obtained from the Director of Technology. Users may not offer, provide, or purchase products or services through the schools' data system unless a special waiver is granted.
5. Users may not use the webpages for political lobbying. The webpages may not be used to support a candidate or to express opinions on political issues.
6. Users will not plagiarize works that they find on the Internet or from other sources. An exception is reposting articles from the ***Danville Advocate Messenger*** since permission has been granted.
7. Access to the webpage is a privilege not a right. Inappropriate use will result in suspension of privileges as well as disciplinary action. District personnel have the authority to determine whether or not content is appropriate.

Social Networking

- 1 In order for District employees to utilize a professional social networking site/account (Twitter, Facebook, Instagram, webpage, etc.) for instructional purposes, they shall comply with the following:
 - a. They shall request prior permission from the building principal and the district Communications Coordinator.
 - b. If permission is granted, staff members will set up the site/account following any district/school guidelines. Guidelines may specify whether access to the site must be given to school/District technology staff.
 - c. Once the site/account has been created, staff members are responsible for monitoring and managing it to promote safe and acceptable use. This includes coaches who might have a parent managing a team account. If this is the case, a coach must also have admin access to the account.
 - d. All social media communications between staff and students must be related to school activities only (coursework, school events, athletic activities, etc.).
 - e. Social media posts intended for students should be formal and professional in tone and language, and should not include photos or images unrelated to the professional purpose of the communication.
 - f. All private social media communications (Twitter direct message, Facebook messenger Instagram message, etc.) with students under a staff member's professional account(s) is discouraged except when absolutely necessary and should always include another staff member or the student's parent/guardian.
 - g. Social media communications may never include confidential information about other students or staff.
 - h. Upon leaving the district and/or current position, staff members must either deactivate professional accounts or transfer ownership to an appropriate staff member.
- 2 Staff use of personal social media must be kept completely separate from employment-related social media. Staff members are prohibited from "friending" or connecting with students using **personal** social media accounts.
- 3 Direct, individual texting with students is discouraged except when absolutely necessary and should always include another staff member or the student's parent/guardian.
- 4 Unsolicited communications from students that do not relate to legitimate school matters must be reported to school or district superiors.
- 5 Staff should not use district or personal devices such as cell phones or computers to access or update **personal** social networking sites during the school day.

All employees shall be subject to disciplinary action if their conduct relating to use of technology or online resources violates this policy or other applicable policy, statutory or regulatory provisions governing employee conduct. The Professional Code of Ethics for Kentucky School Certified Personnel requires certified staff to protect the health, safety, and emotional well-being of students and confidentiality of student information. Conduct in violation of this Code, including, but not limited to, such conduct relating to the use of technology or online resources, must be reported to the Education Professional Standards Board (EPSB) as required by law and may form the basis for disciplinary action up to and including termination.

As an employee of the Danville Schools, I have read and agree to the above Acceptable Use Policy.

Employee Name (Print): _____

Date: _____

Employee Signature: _____

Date: _____