

**EDGERTON LOCAL SCHOOLS  
NETWORK PRIVACY AND ACCEPTABLE USE POLICY  
STAFF MEMBERS**

It is the intention of the Edgerton Local Schools Board of Education to protect the privacy of staff members who use the school computers, computer network, and electronic messaging system to the maximum extent possible given the operational and security need of the District. The purpose of this policy is to identify the limitations on this privacy and the general restrictions applying to the use of computers and electronic messaging system of the District

**ACCEPTABLE AND UNACCEPTABLE USE**

The computer, computer network and messaging systems of the school district are intended for educational uses and work related communication. Incidental use of the email and voice mail system by staff members for personal communication is permitted as long as such communications are limited in number, are initiated during non-work periods, and do not interfere with the primary intended uses of the system.

The following are uses which are unacceptable under any circumstances:

- The transmission of any language or images which are of a graphic sexual nature or depicting murder, death and/or suicide in an inhuman way.
- Please seek guidance from administration regarding the transmission of any materials that may not be suitable for school age children
- The transmission of jokes, pictures, or other material which are obscene, lewd, vulgar, or disparaging of persons based on race, color, sex, age, religion, national origin, or sexual orientation
- The transmission of messages of any other content which would be perceived by a reasonable person to be harassing or threatening
- The connection of any wireless device to the computer network unless specifically authorized by the district's network administrator
- Uses that constitutes defamation (libel or slander)
- Uses that violate copyright laws
- Uses that attempt to gain unauthorized access to another computer system or to impair the operation of another computer system (for example, the transmission of a computer virus or an excessively large e-mail attachment)
- Any commercial for profit-making activities
- Any fundraising activity, unless authorized by an administrator

## **SOCIAL MEDIA**

All Access to Social Networking sites are prohibited during school hours. An employee's personal or private use of social media, such as Facebook, Twitter, blogs, etc., may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

1. Employees shall not post confidential information about students, employees or school system business.
2. Employees shall not list current students as "friends" on social networking sites.
3. Employees shall not knowingly allow students access to their personal social networking sites that discuss or portray sex, nudity, alcohol or drug use or other behaviors associated with the employees' private lives that would be inappropriate to discuss with a student at school.
4. Employees may not knowingly grant students access to any portions of their personal social networking sites that are not accessible to the general public.
5. Employees shall be professional in all internet postings related to or referencing the school system, students and other employees.
6. Employees shall not use profane, pornographic, obscene, indecent, lewd, vulgar or sexually offensive language, pictures or graphics or other communication that could reasonably be anticipated to cause a substantial disruption to the school environment.
7. Employee shall not use the school system's logo or other copyrighted material of the system without express, written consent from the board.
8. Employees shall not post identifiable images of a student or student's family without permission from the student and the student's parent or legal guardian.
9. Employees shall not use internet postings to libel or defame the board, individual board members, students or other school employees.
10. Employees shall not use internet postings to harass, bully or intimidate other employees or students in violation of policy 1710/4021/7230, Prohibition Against Discrimination, Harassment and Bullying, or state and federal laws.
11. Employees shall not post inappropriate content that negatively impacts their ability to perform their jobs.
12. Employees shall not use internet postings to engage in any other conduct that violates board policy and administrative procedures or state and federal laws.

## **DISTRICT APPROVED SOCIAL MEDIA**

- All Facebook, Twitter, Snapchat, blogs or other social media sites used for district purposes are to be created with a district email account.
- The account is to be monitored by the creator or group on a regular basis for inappropriate use or responses.
- In case of hacking or hijacking of the account, the user is to un-publish the account and contact technology.

- Posting of pictures and media will follow guidelines of the district's parent consent approval.
  - No identifiable images
  - No first or last names of students

### **SECURITY AND INTEGRITY**

Staff members shall not take any action which would compromise the security of any computer, network of messaging system. This would include the unauthorized release or sharing of passwords network or wireless and the intentional disabling of any security features of the system.

Staff members shall not take any actions which may adversely affect the integrity, functionality, or reliability of any computer. (for example, the installation of hardware or software not authorized by the district's administrator)

Staff members shall report to the district's network administrator and a School District administrator any action by student or other staff member which would violate the security and integrity of any computer, network, or messaging system whenever such actions become known to them in the normal course of their work duties. **This shall not be construed as creating any liability for staff members for the computer-related misconduct of students or other staff members.**

### **RIGHT OF ACCESS**

Although the Board of Education respects the natural desire of all persons for privacy of the personal communications, and will attempt to preserve this privacy whenever possible, the operational and security needs of the District's computer network and messaging system requires that full access be available at all times. The School District therefore reserves the right to access and inspect any computer, device, or electronic media within its systems and any data, information, and messages which may be contained therein. All such data, information, and messages are the property of the Schools District and staff members should have no expectation that any messages sent or received on or through the School District's system will always remain private.