

## **TECHNOLOGY: Access to and Responsible Use of Technology Resources & Information Databases**

The Edmond Public Schools Access to and Responsible Use of Technology Resources & Information Databases Policy will govern all of the district's computer systems and information databases accessed by all technology users. The term "Users," refers to all technology users and is defined as all staff, students, and individuals provided access to the network. Users will comply with current requirements regarding responsible use of the system and network.

The Edmond Public Schools recognizes that as technologies evolve, the manner in which information may be accessed, communicated, and transferred may alter teaching and learning practices. It is the district's intent to provide reasonable, equitable, and safe access to and storage of information for both employees and students. As in all of its work with and for students and families, the Family Educational Rights and Privacy Act (FERPA) guides many of the district's decisions with regard to the wise and judicious use of technology.

### **A. Shared Responsibility**

The district's policy of "Shared Responsibility" means that users are expected to act responsibly in their use of technology resources. Users will strictly adhere to this policy and to the rules and regulations relating to the use of the network or the district's computer systems and will be held accountable for their actions in this regard.

### **B. Networked Information Systems Responsibility**

Access to the district's computer systems and to the network is a privilege, which can be revoked in cases of misuse. The network is provided to users for educationally related communication, research, and/or job related activities. Unauthorized online access, including "hacking" and other unlawful activities, is prohibited.

The users of the network will respect and comply at all times with local, state, federal and international laws governing or relating to their use of the network. The district will cooperate fully with local, state, federal, and international officials in any investigation concerning or relating to any illegal activities conducted through and otherwise involving the district's computer systems.

### **C. Limitation of Liability**

Adopted: 12-07-98  
Revised: 05-06-02  
Revised: 04-07-03  
Revised: 06-07-10  
Revised: 10-01-12  
Revised: 01-09-17  
Revised: 06-04-18

The district uses internet filtering to control and regulate access to internet sites. This does not provide an absolute means for preventing access to inappropriate material and should never take the place of direct supervision in the classroom. If a user inadvertently accesses inappropriate material, or has knowledge of others accessing inappropriate material, the user should immediately inform an administrator.

#### **D. System Security & Internet Safety**

Failure to secure a computer for even a short period of time can have significant consequences. Users are responsible for their user ID accounts and passwords and should take reasonable precautions to prevent others from gaining access to their accounts. Users are solely responsible for all actions taken under their user ID. All staff members are expected to lock their workstations when away from them for even a moment.

Sharing a user ID or password with any other person is prohibited. Under no circumstances may users provide their passwords to another person or permit another person to use their account once activated.

Users should never give out private or confidential information about themselves or others on the internet. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors is strictly prohibited.

For the protection and security of Edmond Public Schools' networked system, it is prohibited to directly attach any network device, such as a wireless access point, to the Edmond Public Schools' network or to create a personal wireless network while on campus.

When using the internet for class activities, teachers will select material that is age appropriate and relevant to the course objectives. Teachers will review the material and internet sites they require or recommend students access in order to determine the appropriateness of the material. Teachers also should be mindful of the regulations and restrictions regarding the posting of student pictures and personal information on web pages and other internet accessible resources.

#### **E. Respecting Resource Limits**

The district network system should be used for educational and professional or career development activities.

Users are responsible for the contents of their home directory. Only school or work related materials may be stored in a user's home directory or any other district approved storage

Adopted: 12-07-98  
Revised: 05-06-02  
Revised: 04-07-03  
Revised: 06-07-10  
Revised: 10-01-12  
Revised: 01-09-17  
Revised: 06-04-18

systems. Given the finite level of the district networked storage space, users are expected to limit downloads of any size to work-related files.

#### **F. Copyright and Plagiarism**

United States copyright law will govern the use of material accessed through the network. Employees and students will make a standard practice of requesting permission from the holder of a work before copying material or incorporating substantial portions of a work in other materials. This does not apply to appropriately cited references in scholarly research.

Employees who violate this provision do so at their own risk and will be held personally liable for their negligence.

#### **G. Active Restriction Measures**

To comply with the Child Internet Protection Act (CIPA) and other federal and state statutes, the school district will utilize filtering software or other technologies to protect users from accessing visual depictions that are obscene, pornographic, or harmful to minors.

#### **H. Education of Users in Appropriate Online Behaviors**

Each school's instructional staff is responsible for instructing students in the appropriate use of technology before allowing them on the network. Users will be educated about safe and appropriate online behavior, including interactions with other individuals on email, messaging, and social networking websites in an effort to assure their safe and secure use of direct electronic communications on the district network. In addition, cyberbullying awareness and response will be addressed in student handbooks and classroom instruction.

In the classroom and other learning spaces, student use of the internet should be related to specific learning objectives. All staff, including teachers, support, and administration, are responsible for monitoring student activity on the school network. Within the learning environment, the staff member assigned to a student or group of students is responsible for monitoring their use of the network and internet

#### **I. Use of Personal/District Technology**

All EPS resources are intended for instructional and job related activities. Personal computing devices and software are permitted, as long as this policy, the Technology Standards of Conduct, and all site rules and procedures are followed. Personal computing devices and software will not be supported by the district nor will the district be held financially liable for loss or damage of said equipment or software. Personal data, images, other media, or software may be removed from district technology at the discretion of the district, as required to properly maintain district resources.

Adopted: 12-07-98  
Revised: 05-06-02  
Revised: 04-07-03  
Revised: 06-07-10  
Revised: 10-01-12  
Revised: 01-09-17  
Revised: 06-04-18

Teachers must ensure that all students are able to participate in classroom activities and assignments that require a mobile device.

The superintendent/designee is responsible for developing/maintaining procedures specific for the use, care, inventory and tracking of district provided wireless devices. This includes those district-owned devices that are distributed to students for their individual use as an educational tool.

### **1. Staff Use of Technology**

#### a. General use of district telecommunication devices:

1) The Board of Education recognizes that the use of telecommunications is important for communicating with parents, vendors and others in conducting school business. Timely and appropriate use (effective, efficient, ethical and lawful) is expected.

#### b. Use of district IP telephone equipment:

1) Use of the district IP phone system for personal business is strongly discouraged and is to be limited to times that do not interfere with or detract from the employee's work functions.

2) Long distance calls are sometimes required in conducting school business. The superintendent/designee is responsible for developing/maintaining procedures for authorizing and tracking long distance use, when appropriate. Employees are prohibited from making long distance calls for personal business at district expense.

#### c. Wireless devices:

1) For the purpose of this policy, wireless devices are deemed to include all mobile phones, laptop/tablets, two-way radios, and other devices that use Wi-Fi or radio frequencies for communication. While wireless devices are at times assigned to employees for conducting school business, other staff members may also possess wireless communication devices while on school premises. The usage of these devices is governed by this policy. The above-stated "General Use" provisions also apply to employee use of wireless communication devices. Use of wireless devices for personal business during the workday is discouraged and is to be limited to times that do not interfere with or detract from employees' work functions.

2) Employees who choose to bring personal wireless devices to school do so at their own risk. Edmond Public Schools is not responsible for the theft or loss of personal wireless devices.

## **2. Student Use of Technology**

### **a. Wireless Devices**

1) The Edmond Public Schools' policy on wireless devices is designed to ensure that their use does not interfere with, but enhances, the learning experience. Wireless devices are deemed to include all mobile phones, laptop/tablets, and other devices that use Wi-Fi or radio frequencies for communication.

2) Students who choose to bring personal wireless devices to school do so at their own risk. Edmond Public Schools is not responsible for the theft or loss of personal wireless devices.

3) Students may also use district owned wireless devices. They will be responsible for the safe, responsible, and appropriate use of the devices at all times.

4) Specifics as to student use and responsibility for district-owned devices, wireless and otherwise, will be delineated, explained, and agreed upon by students and their families prior to assignment of the devices through uniform district-led and site implemented procedures.

5) Student use of cell phones or other personal electronic devices on campus during the school day is a privilege. Cell phones, their use and all functions within a cell phone (i.e., camera and all other applications) are prohibited from use in classrooms and media centers and any other area in which academic work is in progress, including student productions such as plays and concerts. Student assemblies, such as those held for pep rallies and charity weeks, may include appropriate opportunities for exceptions to the phone-free learning zone. All student cell phones should be stored, secured and out of sight in a locker, backpack, purse or pocket during class time.

At high schools, cell phones may be used by students before school, between classes, lunch and after school on campus. At middle and elementary schools, students may possess phones; however, they must be turned off during school hours.

6) Specific guidelines and expectations for student use of technology are illuminated in the regulations that accompany this policy.

## **J. No Expectation of Privacy**

No student or employee shall have any expectation of privacy in any computer usage, electronic mail being sent or received by the district's computers or district-provided internet access. The district's system operators may access any electronic mail or computer usage and may delete any inappropriate material found, sent or received using the district's computers or district-provided internet access. In addition, discipline may be imposed for improper usage.

## **K. Consequences for Violations**

Adopted: 12-07-98

Revised: 05-06-02

Revised: 04-07-03

Revised: 06-07-10

Revised: 10-01-12

Revised: 01-09-17

Revised: 06-04-18

Consequences will be determined based upon the type of violation, past history, and level of the user. Certain violations for misuse of technology may lead to additional, more severe penalties and legal action, as applicable. If the district becomes aware that a user may have violated the law or board policy, an individual search of the user's files, internet usage, or other electronic/digital media will be conducted. Seizure of the device may also be expected. The investigation and its scope will be reasonable, calculated to disclose the existence and nature of the alleged violation.

Penalties for violations may include, but are not limited to:

1. Loss of internet access and/or network access, for a determined amount of time according to the offense.
2. Staff misuse of technology may result in disciplinary measures to include dismissal.
3. Student offenses will include notifying the student's parent/guardian of an incident and possible disciplinary action appropriate to the severity of the offense.