

EMPLOYEE USE OF TECHNOLOGY

The District provides employees with access to and use of a variety of information technology resources in an effort to allow them to be more efficient, creative, productive and have information that is necessary for them to carry out their responsibilities as district employees. Employees are expected and required to use these information technology resources in a manner consistent with their positions and work responsibilities with the district.

For purposes of board policy, information technology resources include, but are not limited to, fax machines, printers, software applications, Internet access, voice mail, electronic mail (e-mail), desk/lap top computers, scanners, multi-media equipment, terminals, telephones, copy machines and data networks. The policy provides guidance to employees in the following, among other areas:

Software Use/Duplication – Only work-related software is to be used on district computers. No personal software, even if bought by an individual specifically for classroom/office use, may be installed and used without prior authorization from the building administrator. This applies to, but is not limited to, games, utilities and communication software. District employees are expected to comply with all copyright and plagiarism laws that protect commercially purchased software. The copying and duplication of software for any reason is expressly prohibited. Any software in use on any district computer must be a legally licensed copy. The only exceptions to this policy are demo software, shareware and freeware. Software such as these must be checked for viruses by the employee before being used.

Internet Use – Internet access is provided to authorized district employees. Employees are encouraged to use the Internet and the resources found therein for research and instruction for official district activities. The network software and hardware possessed by the district have the capability to monitor Internet activity by users. The network will be configured to prevent employees from visiting sites that are inappropriate and unlikely to be helpful in conducting district business. The district conducts random audits of all Internet activity with the intent of insuring that such activity conforms to district guidelines. Under no circumstances shall an employee, unless directly related to work or unless requested by a building administrator, visit or make repeated attempts to visit any Internet site that is educationally inappropriate. These sites include, but are not limited to: pornographic sites, sites with nudity, gambling sites and sites that deal with illegal activity.

Email System Use – The e-mail system is the property of the district and is provided to employees to assist them in conducting district business. Email of a personal nature should not be used during the student contact time (if a teacher) or work-related times (if a classified employee). All messages composed, sent or received on the email system are and remain the property of the district. The district reserves the right to monitor the e-mail system in order to ensure that it is being used for approved purposes only and to ensure that district policies are being followed. Employees do not have a personal privacy right to any material created, store or sent from the district e-mail system. E-mail is not secure. Employees are prohibited from sending e-mail or otherwise using the e-mail system in connection with any of, but not limited to, the following activities:

1. Engaging in personal business or entertainment outside of approved times.
2. Engaging in illegal, fraudulent or malicious activities.

3. Sending or storing offensive, discriminatory, disruptive, obscene or defamatory material.
4. Annoying or harassing other persons.
5. Using another individual's account or identity without explicit authorization.
6. Attempting to test circumvents or defeat security/auditing systems without prior authorization.
7. Sending out mass e-mail messages with the intent of disrupting the e-mail system.
8. Sending non-work related attachments.
9. Accessing/retrieving or reading e-mail messages sent to other individuals without authorization.
10. Permitting unauthorized individuals to access the district's e-mail system.

Other Information Technology Resource Use – The use of technology resources for personal use of any kind is not permitted without authorization of the building administrator. Examples of unacceptable use include, but are not limited to:

1. Transmitting or distributing material that is confidential to the district.
2. Disrupting network services, such as distributing computer viruses.
3. Intercepting or altering the network.
4. Reproduction and/or distribution of copyrighted materials without appropriate authorization.

Inappropriate use of the district's technology resources may result in discipline.