

Technology Ethics

Unless specified otherwise, these procedures apply equally to students, teachers, administrators, and contractors employed by the district. Teachers and network administrators may have extra responsibilities owing to the nature of their position and/or access privileges.

Users of technological equipment and the information contained in them and generated by the use of such equipment should be aware that the district will uphold rigorously the laws pertaining to the equipment and the use of the information associated with them. The district may prosecute to the fullest extent of the law anyone caught violating such laws.

A. Privacy

Everyone has the right to prohibit the unauthorized accessing of information they create or are entrusted with, including electronic mail. No one shall access, view or use private information without the consent of its author or guardian. If a person is unsure about whether or not information is private, the person should assume it is private and get clear permission before accessing the information. No one is to alter private workstation areas or desktop environments without the consent of the assigned user.

NOTE: in cases involving activity prohibited by district policy and/or law, the above privacy rights do not protect an individual from discipline and/or prosecution.

B. Use of Copyrighted Software

Software users shall abide by the software licensing agreements provided by software publishers. For copyrighted software, the licensee shall retain the license agreement and make it available upon request. For licensed software, the licensee shall retain the master disks and make them available upon request. Without notice, any equipment on district premises may be audited for compliance. Software piracy, the illegal use or possession of copyrighted software, is strictly prohibited.

C. Site Licensed Software

Site licensed software is software which can be used on any equipment at the site for which the software was purchased. This software can be copied legally by anyone to any equipment at the site belonging to the licensee. Unless permitted by the license, it shall not be copied to equipment not owned by the licensee. Before equipment is moved from one site to another, any site licensed software shall be removed.

D. Limited Use Software

Limited use software is that purchased for use by a limited number of concurrent users. This software is launched from a server, and concurrent use is regulated by server software. Unless permitted by the license, this software shall not be copied off of the server to individual hard drives or storage devices.

E. Single License Software

Single license software can be owned by a school, a department or sub-organization within the district. Such software shall not be copied to multiple machines or media in violation of the license agreement. Such software owned by individuals in the district may be brought into the district under the following conditions:

1. The user can prove ownership.
2. The user adheres to the licensing agreement for that software.

3. The user has registered the software with the software company.

F. Property Rights

People and organizations who own equipment have the right to specify who uses the equipment or services, under what circumstances, and to what purpose. The following property rights apply:

1. No one shall steal, vandalize, or alter equipment.
2. No one shall use equipment belonging to someone else except as permitted by the owner.
3. Equipment purchased by the district or an organization within the district (such as a PTA) belongs to the district or purchasing sub-organization. Teachers, administrators and students in the district do not have ownership rights to equipment loaned to them by the district.
4. Equipment purchased with district funds is intended for use by students and teachers alike. No one is conferred exclusive use of district equipment unless authorized by the superintendent.

G. Data Security and Liability

Data security is the assurance that private information cannot be viewed or altered by unauthorized persons. To reasonably ensure such security, users shall abide by the following:

1. No one shall put private information in a public directory or otherwise decrease a public directory's intended security level.
2. No one shall use or distribute someone else's private password.
3. Everyone using a network is responsible for safeguarding the privacy of their password and, by extension, the privacy of the entire network.
4. Users should change passwords regularly and not use words or names which could be guessed (combining letters and numbers helps to foil attempts at guessing).
5. Each person is responsible for making backup copies of documents critical to them.

While the servers will be backed up on a regular basis, the district assumes no responsibility or liability if documents stored on district equipment are lost or damaged. The district is not responsible for security violations beyond the proper punishment of those caught. That is, if someone is harmed because a password was stolen or guessed, the district is not responsible or liable.