



Irvine Unified School District

TECHNOLOGICAL RESOURCES ACCEPTABLE USE POLICY

IUSD supports access by students and staff to rich information and technological resources, and encourages staff and students to develop the information research and technological skills necessary to use such resources effectively. The District's technological resources include the computer network, web sites, Internet access, e-mail, voice mail, video, and telephone systems. Technological resources are provided for students and staff to collaborate, produce, publish, conduct research, and communicate with others on a local, national, and international level. In return, every IUSD user is expected to use these resources primarily for educational or job-related purposes. Personal activities will be limited and will in no way interfere with the educational/professional time and use for which the resources are intended. All users will act in a responsible, ethical, and legal manner and conform to common etiquette that includes being polite, using appropriate language, and respecting privacy.

The Irvine Unified School District's computer network provides access to electronic resources and to the Internet. Similar to the Library Bill of Rights, the Irvine Unified School District holds that a person's right to access Internet and other technological resources should not be denied or abridged because of origin, age, background or views.

IUSD has taken reasonable steps to ensure that its technological resources are used only for activities that support the curriculum or one's professional role. Users should not expect privacy through e-mail, Internet usage, or created documents. IUSD will monitor individual use of all technological systems as needed. However, total security on such a far reaching system is imperfect and impossible to achieve. Realistically, school computers and other technological resources can be used inappropriately, if one is persistent. Using any IUSD technological system is a privilege that may be revoked at any time for unacceptable conduct. Unacceptable conduct includes the following:

1. Using technological resources for illegal or unethical activities, including plagiarism, copyright or contract violations
2. Using technological resources for financial or commercial gain
3. Using technological resources for advocating for ballot measures or political candidates without Board approval
4. Accessing or exploring on-line locations, materials or on-line games that do not support the curriculum and/or are inappropriate for school-related work
5. Downloading, installing, or executing unlicensed or unauthorized software, including viruses
6. Vandalizing and/or tampering with equipment, programs, files, system performance or other components of the network, including copying, distributing, or modifying copyrighted software
7. Causing congestion on any technological system or interfering with the work of others -
- e.g., engaging in chain letters, unapproved chat rooms, or in peer-to-peer networking applications, such as Napster, Gnutella, etc, broadcasting messages to lists or individuals, modifying or deleting files

8. Attempting to infiltrate, or "hack" into any technological system, or interfering with another person's ability to use that system, including password sniffing, using a keylogger, and/or port scanning
9. Sending, or receiving materials/emails that a) are pornographic or obscene in nature, b) purport to offer, arrange for, or negotiate the use or sale of drugs or alcohol, c) harass, intimidate, or threaten others, or d) incite others to acts of violence, bullying, or harassment
10. Using unauthorized fee-based services on the Internet
11. Intentionally wasting finite resources -- e.g., on-line games, instant messaging
12. Gaining unauthorized access to any technological system
13. Revealing the home address or phone number of another person, or, if a student, revealing one's own home address or phone number
14. Invading or violating the privacy of other individuals and/or their information
15. Using another user's account or user name or allowing another user access to one's own account or user name
16. Sharing one's password either knowingly or carelessly, or failing to conform to IUSD directives for password change and creation
17. Coaching, helping, observing or joining any unauthorized activity on any technological system
18. Using e-mail, as a student, for other than school-related purposes
19. Posting anonymous messages, unapproved web pages, or unlawful or libelous information on the system
20. Encrypting files or restricting files through unauthorized password protection
21. Engaging in sexual harassment or other objectionable activities in public or private messages -- e.g., activities that are abusive, sexually explicit, threatening, demeaning or using objectionable language
22. Falsifying permission, authorization or identification documents.
23. Granting remote or local control of a networked system to a third party.
24. Using any computer or wireless device on the IUSD network to gain access to another computer including remotely accessing an offsite or home computer.

Violations of the Technological Resources Acceptable Use Policy, or any willful act designed to disrupt any technological system, will result in disciplinary action up to and including suspension or expulsion, and/or legal action, and may also result in a loss of access to the system or various elements of the system.

Parent(s) and guardian(s) are responsible for setting the standards for members of their family. Therefore, we support the right of each family to select or refuse Internet access for their student.

[Technology Resources Acceptable Use Agreement](#)

Board Policy 6163.4 Adopted: October 16, 2001
Revised: August 27, 2002
Reference: California Penal Code, Section 502