

# Acceptable Use Policies



Written by [Jim Peterson](#), [Bloomington School District](#), Bloomington, IL

---

## Introduction

Although the installation of filters, desktop and network security packages, firewalls and other hardware and software are important in protecting users from technology ailments and misuse, issues arise with information technology in schools that cannot be controlled by hardware and software alone. When most school districts install networked computers, and connect them to the Internet, there is a specific purpose in mind: to enhance the educational opportunities and resources for its staff and students. An acceptable use policy is a standard document that allows the district to outline the rights, responsibilities and governance of its network. The purpose of this paper is to explore the components of acceptable use policies and the ethical questions that they raise.

---

## Acceptable Use Policy Components

Many of the Acceptable Use Policies adopted by boards of education are modeled after University and college level acceptable use policies. According to the National Center for Education Statistics, a properly designed acceptable use policy should include the following:

- Individual rights regarding access to the system and to resources obtained through use of the system.
- Individual responsibilities with regard to the system, its contents and connections obtained through the system.
- Rights of the organization relating to the system and access.
- Organizational responsibilities.

In designing an Acceptable Use Policy, many districts find it beneficial to involve an array of partners in the development, including board members, administration and staff. This is important in not only providing input in the policy, but building a knowledge base with a core group of individuals - individuals who will eventually be involved in its dissemination and enforcement. Often, schools/districts will develop one acceptable use policy for all users, while others will develop separate policies for staff and students. Once a policy is approved by the board of education, collective bargaining units, or other entities, the policy is distributed to all staff and students for their signature of acceptance prior to using the network resources. Students are often required to provide the signature of their parent or guardian.

## Outlining Terms and Conditions

Most acceptable use policies begin by outlining the terms and conditions of the policy, including:

**Acceptable Use** - in this section a broad-based definition is provided on what is considered acceptable network use. Common language includes "the purpose of the network/Internet is for the purpose of education, communication or research and be consistent with the educational objectives of the school/district as set forth in written board policy."

**Privileges** - this section is used to make a statement about the privilege of network use, the right to revoke privileges, and the designation of authorities to revoke such privileges. Common language includes "Network use is a privilege and not a right. Inappropriate use may result in a cancellation of privileges. School staff member, usually a technology coordinator or building principal, will make all decisions regarding whether or not a user has violated the AUP and may deny, revoke or suspend access at any time."

**Due Process** - this section is to included for those users who may question the revoking of privileges. Common language includes "Users who disagree with the decision made regarding whether or not an employee has violated the AUP may appeal such decision through grievance procedures of collective bargaining agreement."

**Unacceptable Use** - this section is often included to demonstrate examples of unacceptable use. Common language includes "Unacceptable use should be defined but not limited to, nor attempt to state all required or prescribed behaviors by users. Examples of such include:

- Intentionally using the network for illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;
- Downloading copyrighted material for other than person use (personal use includes fair use in the classroom) without permission; commercial use;
- Using the network for commercial gain;
- Invading the privacy of individuals;
- Using another user's account or password without that user's permission;
- Intentionally posting of material authored or created by another without his/her consent;
- Intentionally posting of anonymous messages;
- Accessing, submitting, posting, publishing or displaying defamatory, abusive, obscene, profane, pornographic, threatening, racially offensive, harrassing or illegal materials and material of a sexual nature that is inappropriate in a school environment;
- Using the network while access privileges are suspended or revoked."

**Personal Use** - A personal use clause is often included to encourage and facilitate the use of network technology by users. Common language includes "For purposes consistent with this policy; employees are permitted reasonable use of the network for personl use provided that such personal use does not interfere with or disrupt the educational process or the normal operation of the school/district and that such personal use does not violate any of the policy provisions."

**Training** - Many schools find it important to include the degree of staff training that will be provided in the use of the network and acquaint employees with the policy.

**General Conditions and Information** - Often, the acceptable use policy will also include general statements of conditions and information about the network within the acceptable use policy. Common elements and language include:

**No Warranties** - the school/district makes no warranties of any kind, whether expressed or implied, for the service it provides and will not be responsible for any damages an individual suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries or service interruptions caused by unforeseen network problems or a user's errors or omissions. Use of any information obtained via the Internet is at a user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

**Unauthorized Access** - Users shall not tamper with or attempt to gain access to computer data for which the employee has no security authorization. This includes, but is not limited to, financial, employee, or student information. If the security level of a user is in doubt, he/she is to contact the appropriate administration.

**Network Etiquette** - Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- be polite. He/she should not become abusive in her/her messages to others
- use appropriate language. Individuals should not swear, use vulgarities or any other inappropriate language.
- not reveal the personal information of other users
- recognize that electronic mail is not private
- not use the network in any way that would disrupt its use by others.

**Vandalism** - Vandalism is defined as any malicious attempt to harm or destroy data of another user or any network. This includes, but is not limited to, the uploading or creation of computer viruses.

**Security** - Network security is of high priority. If a user can identify a security lapse, the user must notify administration.

**Violation of Policies** - Any user who violates the policy shall be subject to disciplinary action including, but not limited to, written warnings, suspension without pay, or dismissal in accordance with the applicable provisions of the appropriate entity agreements or school code. In addition, if a user's conduct violates federal or state laws, the user may be subject to prosecution under such laws.

---

## Issues

### Vague Language

As one may note from the examples of acceptable use policy components above, the language of acceptable use policies is broad-based and not entirely specific. Particular phrases, such as "including, but not limited to" or terms, like "inappropriate", that are embedded throughout the acceptable use policy are often considered vague. This is often used as a protection for the school to include an array of technology misuse instances - especially those that have yet to be defined. This often becomes a point of

contention with users who may violate such policies as illustrated by a number of cases in state and federal courts. In the words of Nancy Willard, author of [K-12 Acceptable Use Policies](#), "Rules that do not provide sufficient clarity can be attacked on the grounds that they are unconstitutionally vague. Courts have declined to apply criminal standards for the determination of vagueness in the educational environment because it is recognized that school officials need flexibility to respond to the unexpected and school sanctions do not reach the level of criminal sanctions. Courts have upheld as sufficiently clear such terms as "willful disobedience", intentional disruption", and "vulgarity" in a school setting."

---

### **Annotated Web Sites**

[K-12 Internet Acceptable Use Policies](#) (<http://www.erehwon.com/k12aup/>) by Nancy Willard

This site provides a legal and educational analysis of K12 Acceptable Use Policies. It also includes a number of templates for each aspect in the development and implementation of AUPs, including:

- Student Acceptable Use Policy Template
- Student Account Agreement Template
- Employee Account Agreement Template
- Guest Account Agreement Template
- Letter to Parents Template

[Armadillo's Web Server](#) (<http://www.rice.edu/armadillo/acceptable.html>)

This site is a clearinghouse of information about K12 acceptable use policies, including examples, discussions and whitepapers, and various challenges to acceptable use policies in the courts.

[National Center for Education Statistics](#) (<http://nces.ed.gov/pubs98/safetech/appendix-d.html>)

This appendix provides samples have been compiled from existing agreements that are currently in use in schools and local education agencies.

---

Return to [Educator's Guide to Computer Crime and Technology Misuse](#)

Developed 3/5/99. Last modified 5/4/99.

---