



Internet Acceptable Use Policy Best Practices for K-12

Issued by the M86 Marketing Department

Introduction

M86 Security's solutions are used extensively throughout the education sector for Internet filtering and reporting. Through our partnerships, we have learned and collaborated with some of the most innovative IT administrators in education. In an effort to understand the importance of implementing **Internet Acceptable Use Policies (AUPs)** within Education, M86 turned to Jim Culbert. As the Information Security Analyst at Duval County Public Schools (FL), Mr. Culbert is regarded as an expert in enforcing measures for online safety. Named a *THE Journal* "2006 Innovator" in Education, Mr. Culbert's approach to online safety is the framework for this best practices guide.

In addition, we have made available several K-12 focused templates and documents that can assist you in executing the practices illustrated in this guide at www.m86security.com/solutions/industry_solutions/acceptable-use-policies.asp.

The Importance of Internet Acceptable Use Policies

In today's modern classroom, educators and students utilize shared instructional resources such as the Internet and school-wide computer networks as frequently as they do books. Due to the increasing use of these educational tools, administrators must take steps to maintain their appropriate use in the K-12 environment in order to ensure student safety, preserve network bandwidth and limit expense. In addition, the Children's Internet Protection Act (CIPA) requires schools receiving federal E-Rate funds to filter out "unwanted" Internet content, in an attempt to prevent online access to pictures and sites that are obscene, contain child pornography or are harmful to minors. In order to comply with CIPA's provisions, educational organizations are compelled to establish Internet safety guidelines for the appropriate use of computer networks, otherwise known as AUPs.

An AUP is a written agreement signed by teachers, students and their parents that outlines the terms and conditions of Internet use, rules of online behavior, access privileges and penalties for violations of the policy. Anyone using the school's Internet connections should be required to sign the AUP. In addition, schools should consult their attorneys for legal guidance in drafting an AUP. In order to fully detail what is expected for online behavior, Mr. Culbert recommends that strong wording be included in the Student Code of Conduct handbook regarding appropriate and inappropriate use of the Internet.

Creating and enforcing an effective AUP is a collaborative effort and a multi-step process. As Robert Losinski, Information Security Administrator at Denver Public Schools states, "The most effective and enforceable policies are those that are created and agreed upon by the administration, backed up in the student code of conduct and employee handbook, and then monitored and enforced by robust filtering and reporting tools." (*THE Journal*, March 2007)

What Should an Acceptable Use Policy Include?

An Internet AUP should contain the following:

Introduction

- Detail reasons for the policy and what the policy covers

Definitions

- Define key words used in the policy such as "computer network", "Internet", "E-mail" and "chat rooms"
- Define all ambiguous terms, including personal contact information, personal safety and inappropriate Web material

Policy Statement should include:

- How students will be accessing the Internet
- How the Internet will be used in the classroom
- How you will restrict access to inappropriate and harmful materials
- Online etiquette
- Privacy policies
- Liability disclaimer
- Reminder that Internet use is a privilege and not a right

Acceptable Uses

- Specific examples of acceptable uses

Unacceptable Uses

- Specific examples of unacceptable uses

Violation Consequences

- Specific examples of disciplinary action that a student or teacher can expect for violating Web use

Permission Forms

- Require all teachers and students to acknowledge and sign before their account is activated

Internet Safety Plan

In addition to an AUP, school districts should have an Internet Safety Plan in place that documents the technology protection methods used to block and/or filter visual depictions that are obscene, pornographic or in anyway harmful to minors as defined in CIPA.

An Internet Safety Plan should reflect the district's compliance measures and be made available to all parents/guardians and staff. The plan should address:

- Access by minors to inappropriate matter on the Internet and World Wide Web.
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication.
- Unauthorized access, including "hacking" and other unlawful activities by minors online.
- Unauthorized disclosures and dissemination of personal identification information regarding minors.
- Measures designed to restrict access to materials that may be harmful to minors.
- Protection methods used for 1:1 initiatives when laptops are outside the school network.

Consent Requirement

Including the Internet Safety Plan with the AUP Consent Form is an ideal way to encourage parents and teachers to discuss with children the hazards of the Internet and best practices for online safety.

No student should be allowed to access the school district's Internet connection and related resources unless they have filed an AUP Consent Form, signed both by the student and his/her parent(s) or guardian(s).

Logon Banner

All school district computers should have a logon warning banner displayed at all access points upon each logon. The banner should warn authorized and unauthorized users:

- What is considered the proper use of the system.
- The system is being monitored to detect improper use and other illicit activity.
- There is no expectation of privacy while using the system.
- We have included an example template of a logon banner that can be downloaded from www.m86security.com/solutions/industry_solutions/acceptable-use-policies.asp.

Monitoring and Reporting

Once the policies and procedures are in place, the next step is to ensure your school district implements an effective Internet filtering and reporting solution that monitors Internet activity,

detects inappropriate usage and triggers further investigation when necessary. To do this, M86 recommends the following be implemented as a baseline:

Implement Internet Filtering as a Standard Operation Procedure

- Develop a district policy that covers category blocking.
- Create an Internet review committee that is responsible for the category selection.
- Back up your filtering policy with an enforcement policy.
- Follow the policy unconditionally.

Regular Automated Reporting

- Run automated weekly reports on the previous week's Internet activity.
- Develop trend reporting to help identify emerging threats.
- Define justifiable thresholds on when further investigation is required and under what circumstances.
- When a threshold has been met, run a full week's report on the user's activity. Identify the sites accessed before and after the blocked sites, and locate the search terms used in order to determine intent.
- Divide category-reporting groups into "Default", "Reportable" and "Monitor."

"Default"

- This reporting category should include all the categories your school district has decided to block. It is designed to help identify virus activity, malware, phishing attacks and used for trend analysis. Any user that records over 100 hits on a blocked category should trigger further investigation.

"Reportable" (Zero Tolerance)

- This category should include the categories that have been defined by the school district as zero tolerance. For example, regardless of the intention, whether accidental or not, any hit to the "Child Porn" category should trigger further user investigation. Additional categories might also include, but are not limited to:
 - General Porn
 - Proxy
 - Obscene and Tasteless

"Monitor"

- This category should include categories that may not be blocked, but need to be monitored and justified when accessed. These categories might include:
 - Hate Groups
 - Criminal Skills
 - Monitored for:
 - Gang Activity
 - Guns/Weapons
 - Hate

Enforcement

Effective enforcement begins with regular monitoring and reporting, combined with defined policies on what is unacceptable online behavior. Once implemented, violations of the policy should be enforced through standard disciplinary action.

Students and teachers should be aware and understand that violations of the Internet AUP may result in a loss of access as well as other disciplinary or legal action.

The intent of the enforcement should be designed to not only apply disciplinary action but to change Internet behavioral habits and steer students to educationally-focused content.

Available Templates

The following templates have been developed specifically for K-12 and are available to download from www.m86security.com/solutions/industry_solutions/acceptable-use-policies.asp:

- Internet Safety Plan Template
- Logon Banner Template
- Student Acceptable Use Policy Template

About M86 Security

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters

828 West Taft Avenue
Orange, CA 92665
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific

Millennium Centre, Bldg C, Level 1
600 Great South Road
Eilerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 05/10/10