

INFORMATION PAPER  
NOVEMBER 2010

# Acceptable Use Policies:

Creating and Enforcing Guidelines for  
Use of School Technologies



Network solutions for safe online learning

## Table of Contents

What Is an Acceptable Use Policy.....	3
Why an AUP is Necessary .....	3
Goals of Your AUP.....	3
What to Include in Your AUP .....	3
Tips for Enforcing Your AUP .....	4
Lightspeed Solutions.....	5
Setting Use Policies with Lightspeed .....	6
Monitoring Use with Lightspeed .....	6
For More Information.....	8
About Lightspeed Systems .....	8

©2010 Lightspeed Systems

## **What Is an Acceptable Use Policy**

An essential element in any school's technology plan is an Acceptable Use Policy (AUP) that clearly defines how, when, by whom, and for what purpose a school's technological resources are to be utilized. The policy should also clearly state what the consequences of infringement are. For all students, teachers, and staff who use the school technology, an updated Acceptable Use Policy should be read and signed every year. Since the policy should be able to serve as a legal document, a school attorney should also review it.

## **Why an AUP is Necessary**

While the Internet and other technologies offer many educational rewards, they also pose some risks. A proactive AUP policy can help ensure student safety, as well as educate users on how they are expected to utilize school resources in a safe and productive way. It can also help protect your resources from being used in a way that could damage them. An AUP can serve as an early lesson on Internet safety and appropriate online behavior. And it can help the district and administrators impose consequences, or pursue prosecution or termination, for inappropriate use.

## **Goals of Your AUP**

Your AUP serves many purposes. It may be helpful to consider some of the key goals as you draft or revise your Acceptable Use Policies.

1. To set forth clear expectations about proper use of school technology
2. To reflect the school's educational philosophies and values
3. To be flexible and adaptable as guidelines and technologies change
4. To educate students about topics such as netiquette, cyberbullying, and Internet safety
5. To legally protect the school
6. To protect the students and other users

## **What to Include in Your AUP**

Your Acceptable Use Policies should be unique and tailored to your district's technological resources and educational philosophies.

Nevertheless, an Acceptable Use Policy should include at least:

**Introduction** – A listing of the various technologies available in the school and to which this AUP applies. Also, a description of the goals and educational philosophies that the technologies in your school support and definitions of key terminology used in the policy. And finally, a discussion of what the AUP itself is designed for and what it covers.

**Usage Policies** – A discussion of various policies around the use of technologies, including when technologies are to be used by students and staff as well as for what purposes; the issues of copyright and plagiarism as it applies to the Internet; netiquette and appropriate online behavior; privacy policies; and an explanation of the various filtering and monitoring devices that are used on school computers. You should also include any policies about personally-owned devices using school technology.

**BEST PRACTICE:** Include policies for on-campus resources, school-owned mobile devices, and personally-owned devices brought onto the campus.

**Acceptable Uses** – Specific examples of acceptable uses of school technologies, computers, and the Internet.

**Unacceptable Uses** – Specific examples of UNACCEPTABLE uses of school technologies, computers, and the Internet. This should include a discussion of cyberbullying, pornographic images, sexual content, and sexual misconduct. This section should also include guidance for users about to whom they can direct questions or concerns about unacceptable use.

**Monitoring Alert** – Let users know their activity on school computers will be monitored and that misuse will lead to consequences.

**Consequences** – A discussion of the consequences users should expect to face if they break the policy, for both students and staff.

**Liability** – A disclaimer, freeing the school from liabilities that may arise.

**Acceptance** – Signature and date for each user of school technologies, acknowledging that they have read and understood the policy and agree to follow its guidelines.

**BEST PRACTICE:** Your district AUP should be updated, reviewed by legal counsel, and signed by all users annually.

## Tips for Enforcing Your AUP

1. **Select monitoring software with easy-to-read reports.**

Your monitoring software will need to generate reports that are easy enough to be used and understood by non-technical district employees and law enforcement. Ideally, these non-IT individuals can be assigned administrative rights to directly access what they need.

- 2. Monitor use of mobile devices as well as desktop computers.**

Mobile devices taken off the network by users can be especially susceptible to misuse. Utilize mobile filtering for off-network computers to protect your mobile devices from spyware and viruses; to protect your users from inappropriate content; and to monitor use to make sure it's aligned with policies.
- 3. Get before and after snapshot reports.**

If you see misuse and need to adjust a policy, keep a snapshot of key reports before you change anything. Then take another snapshot after making an adjustment. This will allow you to verify that the change is working, and will preserve evidence of misuse should it be needed later.
- 4. Consider letting HR be the content cop.**

Schedule key reports to be sent to specific people in Human Resources (HR) each day. Reviewing these reports will take less than 15 minutes—and helps determine who or what to monitor more closely, including an individual, computer, email address, or IP address. Ideally, this additional monitoring can be initiated directly by the HR staff.
- 5. Watch specific reports.**

Too much data can be overwhelming. Keeping an eye on a few key reports regularly, and then reviewing others less occasionally, can help you balance monitoring with other tasks. Review reports on overall network activity to identify any unusual spikes, and suspicious search-engine queries to easily detect anyone persistently searching for inappropriate content.
- 6. Be patient to accumulate enough data.**

If you suspect misuse, especially serious misuse (such as sexual misconduct), keep an eye on the data, look for patterns in activity and behavior, and wait for a substantial number of occurrences before becoming invasive. This way there's no chance that the content arrived as an "accident" on a user's desktop.
- 7. Preserve reports.**

Export reports to PDF for easy preservation and presentation.
- 8. Present a contrast.**

Give a picture of the network activity for the district as a whole and contrast that to an individual user's activity to show how far out of the norm it is.

**BEST PRACTICE:** Sometimes misuse of school computers isn't just a breach of policy—it's a crime. Properly documenting and preserving evidence can protect your district and aid prosecution.

Whether you, another department, or some combination of departments will be the content cop, these best practices will make the task cleaner and easier. Enforcing an AUP can appear to be a thankless task; however, occasionally it proves to be a really important undertaking.

## Lightspeed Solutions

Enforcing your school AUP is a two-part process:

1. **Policies.** You have to create policies within your filter and other network solutions that mirror your Acceptable Use Policies.
2. **Reporting.** You need to monitor activity to ensure that your AUPs are being followed.

Lightspeed Systems solutions make it easy to create rules for use of school-owned computers, mail servers, and Web browsing. They also provide comprehensive reporting to alert you to potential breaches to those policies, and helps you correct or amend rules.

Our flagship solution, Total Traffic Control is the complete solution for managing your school network's usage, health, and security. With this comprehensive solution you can monitor user activity, ensure Acceptable Use Policies are being followed (on email, the Web, or the desktop—both on the network and off), reduce dangerous and costly security threats, ensure school resources are utilized safely and effectively, and easily view and share critical information with custom reports.

## Setting Use Policies with Lightspeed

Lightspeed solutions allow you to set policies that match your outlined usage. Policies can be granularly controlled, by user, IP, group, computer, and more.

You can set policies for:

- Ability to go online
- Ability to access certain categories of sites (on the network or off)
- Access to the collaborative online site (My Big Campus)
- Access to hosted student email (Campus Mail)
- Ability to download files or programs
- And more

## Monitoring Use with Lightspeed

Lightspeed Systems comprehensive reporting gives you access to information about who, when, where, and how your network is being utilized, so you can adjust Acceptable Use Policies, change allowed usages, review problems and troubleshoot issues, and plan for ongoing needs.

Each product allows you to create custom reports, or view standard reports. These easy-to-understand reports contain information essential to monitoring how users are interacting with your technology.

### Web Access Manager (Content Filter)

- Blocked Content – Review what pages users tried to visit that were blocked by the filter
- URLs visited – Keep an eye on the sites users are accessing
- Search Engine Queries – See what users are searching for

- Traffic by Category – Review overall traffic by content category
- Suspicious Search Queries – See search queries flagged as having potentially inappropriate content
- HR Report – View network activity for a specific user

#### **My Big Campus (Online Collaboration Site)**

- Suspicious Activity - View reports of messages containing profanity, violence, or suicide keywords.
- Suspicious Images - Review uploaded images flagged by the skin-tone scanner
- Uploaded Files - View and access uploaded files by user. Uploaded files are scanned for viruses and content.

#### **Email Manager (Use of School Email)**

- Top Senders/Receivers – Review your top mail users
- Email Archiving—Search for and review archived email records

#### **Network Traffic Manager (Bandwidth and Network Overview)**

- Top Network Users – See who your top users are
- Busiest Protocols – Review the most heavily trafficked protocols

#### **Security Manager (Viruses and Program Inventory)**

- Blocked Programs – View programs users tried to download or execute that were blocked

#### **Campus Mail (Hosted Email Accounts)**

- Suspicious Activity - View reports of messages containing profanity, violence, or suicide keywords.
- Suspicious Images - Review uploaded images flagged by the skin-tone scanner
- Uploaded Files - View and access uploaded files by user. Uploaded files are scanned for viruses and content.

**BEST PRACTICE:** Have key reports sent to you every day. Have the HR report sent directly to HR. Involve other key stakeholders in monitoring use.

## For More Information

Learn more about Acceptable Use Policies, visit our Resource Center:

<http://www.lightspeedsystems.com/resources/>

When an AUP breach is actually a crime:

<http://www.lightspeedsystems.com/resources/Information-Papers/Info-Forensics.aspx>

Or check out these other sites:

[http://www.education-world.com/a\\_curr/curr093.shtml](http://www.education-world.com/a_curr/curr093.shtml)

<http://www.eschoolnews.com/2008/07/23/educators-struggle-with-aup-enforcement/>

## About Lightspeed Systems

Lightspeed Systems Inc., founded in 1999, develops comprehensive network security and management solutions for the education market. We are committed to helping schools operate their networks effectively and efficiently, so educators can provide safe online teaching and learning environments.

Our software is used in more than 2,000 school districts in the United States, the United Kingdom, and Australia to protect more than 6 million students. For the past four years, Lightspeed Systems has been recognized on the Inc. 5,000 list as one of the fastest-growing private companies.

[www.lightspeedsystems.com](http://www.lightspeedsystems.com)