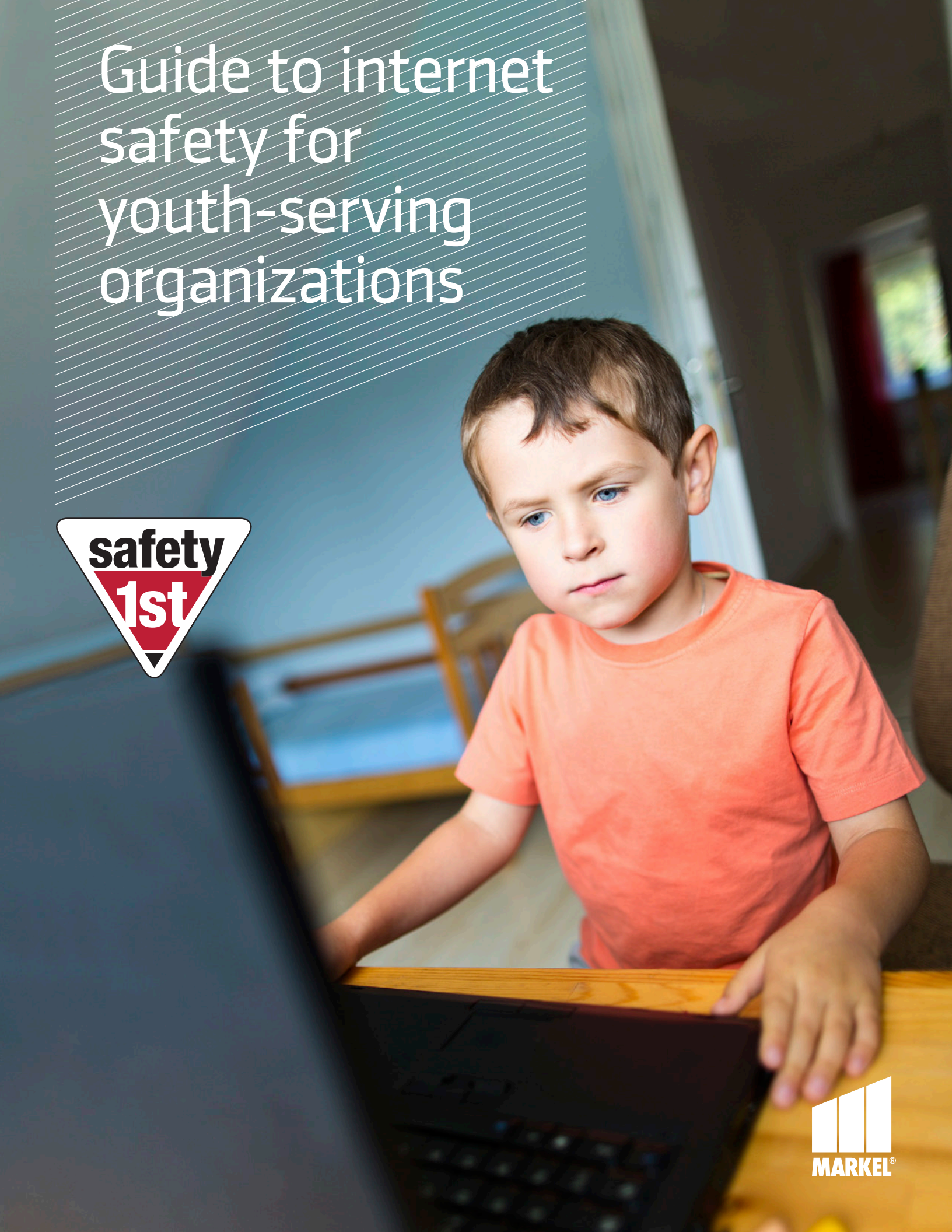
Guide to internet safety for youth-serving organizations



Internet safety for children

By John C. Patterson
Senior Program Director
Nonprofit Risk Management Center

Today, many youth-serving organizations make the internet available to their staff and the children in their programs. Although the internet can be a wonderful learning resource, it can also be a hazardous place for children. This booklet will tell you how to:

- Recognize risks on the internet.
- Prevent internet misuse.
- Establish policies for email and chat room use.
- Write an internet Acceptable Use Policy (IAUP).
- Train staff and children to use the internet safely.
- Assess your organization's web site.
- Protect your organization from liability arising from internet misuse.

This guide also provides a list of online resources you can use to learn more about using the internet safely.

Using the internet

Recognizing risks on the internet

Children face danger on the internet from many fronts. They can view pornographic, violent, and inappropriate web sites with a click of the mouse. But, by far the greatest danger exists in email and chat rooms. There, children can be subjected to harassment, abusive language, and objectionable themes. At worst, unsuspecting children can be duped into revealing personal information to sexual predators, developing an online relationship with them, and ultimately and sometimes tragically, meeting with them. Fortunately, there are some basic steps you can take to protect the children in your care.

Preventing internet misuse

By far the simplest and cheapest way to cut down on internet misuse is by physically locating computers in open, supervised areas. An open location makes it easy for staff to supervise and monitor computer use. Posting your internet use rules where the computers are located also helps reduce internet abuse.

Another quick fix is through software that blocks access to offensive topics found in web sites, news groups, chat rooms, and email. Most programs block access to topics that deal with pornography, illegal activities, drugs, and hate groups. You can also customize the software to block access to topics your organization finds objectionable. Many programs also log all attempts to access blocked topics. No blocking program is 100 percent effective, and children may inadvertently access objectionable web sites and topics. In fact, some children will consider blocking software a personal challenge and try to circumvent it. Staff supervision and monitoring are key to prevent incidents like this from happening. Many of these blocking programs make monitoring internet use easy. All allow you to print reports of web sites visited, and some inform you of internet misuse the instant it happens by sending you an email message. Many also allow you to monitor internet activity as it occurs.

Some highly rated blocking programs are:

- Cyber Patrol - www.cyberpatrol.com
- McAfee Family Protection - www.mcafeefamilyprotection
- PureSight - www.puresight.com

Establishing email and chat room policies

Many organizations give group email accounts to young children and individual accounts to older children and teenagers. Group accounts ensure that young children are supervised while they use the internet.

It's important for children to understand that they must:

- Never give any personal information to anyone they've met online. Personal information includes a child's photo, name, address, age, telephone number, your organization's address, and school name and address.
- Never physically meet with anyone they've met online. If a cyberpal suggests a face-to-face meeting, the child should immediately tell a staff member.
- Never open an email from someone they don't know. Anonymous emails often carry viruses that can harm all the computers on the network.
- Report to a staff member any messages they receive that are harassing, pornographic, or make them feel uneasy.
- Apply the same rules of politeness to email and chat rooms that they use in other forms of communication.

Writing the IAUP

Every youth-serving organization should have an IAUP (Internet Acceptable Use Policy) for two reasons. First, it clearly states your organization's internet use policy for staff and children. Second, it protects your organization from liability arising from intentional internet misuse. Everyone in your program (children, parents, and staff) should receive a copy of your IAUP. The IAUP should contain a sign-off sheet for parents that releases you from liability for their child's intentional misuse of the internet and proves that parents have read, understood, and agreed with your internet use policy.

Most IAUPs cover the following topics:

- Assignment of an internet coordinator (usually the executive director)
- Limitation of liability disclaimer
- Time limits for computer usage
- Acceptable and unacceptable use
- Code of conduct/behavior code
- Penalty for breaking the rules
- Parental notification and responsibilities

Training staff

Your organization's IAUP is a great training tool because it covers every aspect of your internet safety program. Staff should be trained to spot internet abuse on the part of children, as well as how to handle abuses. Staff restrictions, such as no personal use of the internet during business hours and no access to objectionable sites, should also be stressed.

Some directors have been dismissed from their jobs because they accessed pornographic sites-even though they did it on their time off. They were fired because their organization's IAUP clearly stated that access to these and other objectionable sites was forbidden at all times, by all staff members.

Training children

Children, too, will benefit from learning what's in your IAUP. Their training should emphasize your chat room and email policies; children need to know that they must tell a staff member about unwelcome attention as a result of an email message or a chat room session.

Assessing your web site

Your organization's web site is a powerful way to introduce your programs to your community and beyond. Careful selection of your site's content will keep the public interested in your programs and protect children.

Do include:

- Information about your programs.
- Information about your staff's qualifications.
- Kids' artwork and creative writing, signed with first names only, with parental permission (signed release).
- Testimonials and endorsements.
- Group photos of unidentified children.

Don't include:

- Kids' personal information (photos of individual children, names, addresses, ages, schools).

If you feel you must use photos of individual children, get a signed release from their parents before you put the photos out on the internet.

Protecting your organization

As internet use in youth-serving organizations grows, so too does the risk of being sued by parents whose children were sexually abused by someone they met online at your center. Large jury awards are becoming more common in these cases, especially when abuse could have been prevented. In one recent case, a child molester targeted children at a local youth organization, lured them into meeting him, and sexually abused them. The jury found the youth center responsible for the abuse because it did not have the proper safeguards in place to prevent it.

Five steps

Here are five steps you can take today to protect your organization from liability:

1. Instruct children, parents, and staff on acceptable and unacceptable internet use.
2. Post the rules for acceptable usage in a prominent place.
3. Instruct children to report to a staff member all harassing, threatening, or sexually explicit attention they receive through email or in a chat room.
4. Supervise children's use of the internet, especially email and chat rooms.
5. Monitor and record all visits made to prohibited sites and take appropriate action to ensure children don't visit these sites again.

Online Resources

National Center for Missing and Exploited Children

www.missingkids.com

www.missingkids.com/cybertipline

Operates as a resource center and clearinghouse for the public and law enforcement professionals. Focuses attention on sexual exploitation of children on the internet.

Federal Trade Commision

www.ftc.gov/bcp/conline/edcams/kidzprivacy/index.html

Focuses on the issue of kids' privacy online.

KidsCom

www.kidscom.com

Offers a wealth of information on internet safety, including an internet Safety Game.

StopBullying.gov

www.stopbullying.gov/cyberbullying

This site offers resources on what you can do to prevent cyberbullying, and how you can report it when it happens.

It’s all about safety

Safety is your primary goal. It’s ours, too. The best way to keep kids safe is to prevent accidents from happening in the first place. Markel’s Safety 1st education program and risk-management experts can show you how. The program includes:

- Safety guides
- Risk management newsletter series
- Training
- Safety videos and online resources
- Program and facility assessments
- Seminars
- Analysis of loss trends

Please explore our web sites, www.campinsurance.com and www.childcareinsurance.com, to find out more about our programs, or call us at 800-431-1270.

4600 Cox Road
Glen Allen, Virginia 23060
800-431-1270
childcareinsurance.com
campinsurance.com

MARKEL®