Microsoft

Child Online Safety

Key Points

Although the internet enables many enriching experiences for children, there are also risks, including potential exposure to inappropriate content, contact with bullies, and loss of privacy.

The Microsoft approach to children's online safety includes creating innovative technology tools; providing education and guidance; establishing robust internal policies and practices for moderating content and addressing online abuses; and collaborating with nongovernmental organizations, industry, government, and others.

The safety of children online is a community challenge, and government, industry, and others should work together to establish and implement safety principles. As governments address risks associated with new technologies and online services, it is important that they continue to encourage innovation and technology adoption.

Although the internet offers a wealth of positive experiences for children, parents face challenges when monitoring the content their children encounter online, the people they meet there, and what they share.

Inappropriate Content

Young people are curious and may stumble upon inappropriate material (including hateful or sexual content) by clicking a link in email, on a social network, or while searching for something else on the web.

Inappropriate Conduct

Some young people—and adults, too—may use the internet to harass or exploit others. Kids may sometimes broadcast hurtful bullying comments or embarrassing images. A particular concern with mobile devices is sexting—the transmission of sexually explicit photographs and videos taken with a device's camera.

Inappropriate Contact

Adults—and young people, too—use the internet to find and approach vulnerable youth. Frequently, their goal is to develop what young people believe to be meaningful online relationships, a process referred to as "grooming." Grooming can lead to exploitation for sexual purposes or violent or extreme causes.

Inappropriate Commerce

Children can easily fall victim to "phishing" or other scams. They can be enticed to click a flashy ad, open an appealing "free" game, or download a ringtone. These can install viruses, spyware, or other malicious software.

Microsoft Approach

The Microsoft approach to combating child safety issues on the internet includes developing technology, providing education and guidance, establishing internal policies, and partnering with others.

Creating Technology Tools

Microsoft builds safety features into a wide range of its products and services to help parents minimize online risks to their children.

In all editions of the Windows 10 and Windows 8 operating systems, parents can use the Family Safety feature to keep kids safer online, set screen time limits, filter content, and avoid surprise spending.

The Xbox platform is equipped with parental controls to help create a safer environment for all gamers. For example, parents can use Family and Online Safety controls to limit access to games based on age ratings systems like Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI). Bing SafeSearch can help keep adult content in text, images, and videos out of children's search results.

If anyone in the family comes across content or witnesses conduct that violates Microsoft's Code of Conduct, we encourage you to report it using various in-product reporting tools. We all have a role to play in helping to protect our online platforms and services. Reporting these types of concerns to technology companies is essential.

Providing Education and Guidance

The **Microsoft Safer Online website** provides age-based advice for internet use, as well as guidance on issues such as online bullying, identifying misinformation, hate speech, and sexting. Visitors can also learn about **Microsoft's campaign for Digital Civility,** which promotes safer and healthier online interactions.

Establishing Internal Policies and Practices

Microsoft promotes digital safety through robust company-wide policies, standards, and procedures for its web products and services. It enforces policies inherent in its code of conduct for users of its online services, and it moderates content and interactions to address illegal activity, inappropriate material, and other abusive content or conduct.

Partnering with Others

To help promote digital safety for children and young people, Microsoft:

- Developed and shared **PhotoDNA,** a robust image-matching technology that helps nongovernmental organizations, law enforcement, and other technology companies (such as Facebook) find and remove some of the worst images of child sexual abuse from the internet.
- Partnered with The Meet Group, Roblox, Kik, and Thorn to develop a **grooming detection technique** that helps identify potential instances of child online grooming for sexual purposes. This technique builds off Microsoft patented technology and is made freely available via **Thorn**—a technology and child protection nonprofit—to qualified online service companies that offer a chat function.
- Consulted with five governments (Australia, Canada, New Zealand, the UK, and the US) as well as five other companies (Facebook, Google, Roblox, Snapchat, and Twitter) to support the development of the Voluntary Principles to **Counter Online Child Sexual Exploitation and Abuse.**

Policy Considerations

Governments and other policymakers can help promote recent efforts in child online safety by focusing on these priorities:

Strengthen and Enforce Existing Child Protection Laws

Governments must strengthen and enforce laws against the possession and distribution of child sexual abuse images. Microsoft works with the WePROTECT Global Alliance, the UK-based Internet Watch Foundation (IWF), the U.S. National Center for Missing and Exploited Children (NCMEC), INHOPE and other organizations to support government efforts.

Encourage Public-Private Collaboration

Government and industry must collaborate to establish safety principles and offer a more secure online environment for youth. Examples of this collaboration include recommendations from the European Commission to make the internet a safer place for children, the WePROTECT Global Alliance's Model National Response to end child sexual exploitation and abuse online, and the digital citizenship principles published by the Australian Communications and Media Authority (ACMA). As governments address risks associated with new technologies, they must avoid stifling innovation and technology adoption.

Promote Comprehensive Online Safety Education in Schools

Government support for anti-bullying education, as part of a comprehensive online safety curriculum for elementary and secondary school students, can provide a foundation for addressing the problem of online bullying. One example of such support is a US law mandating that anti-bullying measures be taught in any school that receives E-Rate funding from the Federal Communications Commission (FCC). (The E-Rate program gives schools and libraries discounts for telecommunications and internet access).

Support Internet Safety Research

Research is particularly important for identifying factors that increase online risk and for dispelling myths that can lead to misplaced efforts to advance internet safety. Government funding for academic, practical and industry research in these areas is essential.