Microsoft

Family Safety Toolkit

FEBRUARY 2024

TABLE OF CONTENTS

Introduction

What are family safety tools?

Family safety tools are features designed to help parents and caregivers:

1. Engage with their children to help them understand what it means to be online and how to be a good digital citizen.
2. Set guardrails to help guide a child's online activities.

How to use this toolkit

This toolkit provides an overview of some online safety risks and offers general online safety guidance for all ages. Just like any new activity, children benefit from parents and caregivers being actively involved. We encourage families to learn and discuss their online activities together: digital parenting is an active and iterative process. The toolkit draws from resources we have developed over time and our approach is shaped by engagement with young people and in our digital safety partnerships, such as the WeProtect Global Alliance, Tech Coalition, Internet Watch Foundation, and Family Online Safety Institute.

This toolkit also provides guidance on how to leverage Microsoft's safety features and family safety settings to support and enhance your digital parenting. For gaming-specific advice, check out the **Xbox Gaming Safety Toolkit**.

A COUPLE OF TOP-LINE TIPS

Parental controls should not just be 'set and forget'

Instead, they are most effective when integrated into a family-wide approach to safety. Appropriate use of parental controls depends on your family's situation and values – not all children or families are the same. Different families will want to adapt their approach to their technology preferences and the unique needs of their child.

We also encourage open conversations with your child about the use of parental controls.

Being transparent about these tools is important for building trust and showing young people that you respect their privacy. We also recommend talking to them about the user controls they can implement on their own account and why these are important for keeping them safe, especially for teens.

Some Common Online Safety Risks

Our **2024 Global Online Safety Survey** found that 67% of people surveyed were exposed to harmful or offensive material online. Of the teens surveyed (ages 13-17), 70% of them reported having a harmful experience online – teens most commonly encountered misinformation and disinformation, as well as other more personal harms such as cyberbullying, hate speech, and threats of violence. These harmful encounters can result in teens becoming less trusting of other people online, losing sleep, and experiencing lower self-esteem.

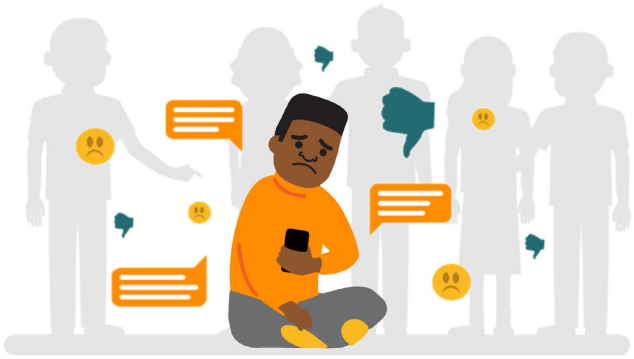
Empowering users to create safe and inclusive online communities enables everyone to participate in digital environments and make the most of the opportunities that technology can bring. For Microsoft, empowerment includes helping people understand the potential online risks and they ways in which they can protect themselves and their families.

This Microsoft Family Safety Toolkit highlights some of the most common online safety risks young people may encounter, including signs that your child may need support. We've included links to a selection of informational resources already made for parents. For example, the **Family Online Safety Institute** (FOSI) offers a **How To Be A Good Digital Parent Toolkit** and **Thorn** has a series of **Discussion Guides** to help you navigate these conversations.

1. Harmful and age-inappropriate content

Harmful and age-inappropriate content refers to any type of media, information, or material that can be harmful or unsuitable for individuals, especially children or teenagers, due to their age or maturity level. Young people may inadvertently come across content that they find concerning or that is intended for a more mature audience.

We recognize that everyone has a different tolerance for content, however, our **Microsoft Code of Conduct** explains what is not allowed and what to expect when accessing our services. We take action to address content that violates our rules – if you or your family sees concerning content, you can report it either in the service or at Microsoft's **Report a Concern**.



2. Bullying and harassment

Cyberbullying and online harassment can be amplified in digital spaces, where content can be sent anonymously, at high volumes, at any time of day. Bullying and harassment may play out, for example, through insults in comments, threatening voice messages, or by publicly sharing embarrassing photos or private messages. Hate speech is a severe form of harassment which may include attacks on personal characteristics, especially things like race, gender identity, sexual orientation, and religion.

Bullying, harassment, and hate speech are prohibited on Microsoft's services and can be reported in the product or **online**. Depending on the service, there may also be options for you to block or mute users.

Cyberbullying and harassment can occur at any age; however, it may be especially damaging to young people, who are more vulnerable to the effects of cyberbullying and online harassment. Our research shows that nearly 41% of teens are worried about cyberbullying and harassment, with teens more concerned than adults. Potential signs of bullying include a child being upset when online or texting or displaying a reluctance to go to, or stay at school, and other activities.

If you are concerned your child may be bullying others, try to speak with them to understand why they are doing this in a non-judgmental way.

It is important to normalize that people make mistakes and focus on connecting with your child to understand what might be contributing to this behavior and to encourage empathy for others.

LEARN MORE

Cyberbullying Research Center

StopBullying.gov

3. Grooming and unwanted content

Unwanted contact can be any online communication a young person finds uncomfortable and could lead them into an unsafe situation. It can come from strangers, online friends or even someone they know in real-life.

Grooming is when predators target individuals for exploitation, which may be sexual in nature. The grooming process typically involves an older person befriending a young person and gaining trust by giving them personal attention. This may involve being highly responsive and flattering or offering material or virtual gifts.

A similar process may also be used by violent extremist recruiters to enlist young people to hate-based causes. Recruiters may look for vulnerable people, including individuals who appear isolated, express loneliness, or have low self-esteem. A common strategy is to suggest a conversation is taken off a platform to a different space, such as an encrypted messaging app.

Signs may include changes in mood or behavior, becoming withdrawn, or receiving unexpected gifts or money. Teach them to trust their instincts about when a request seems concerning or uncomfortable (e.g., if a person asks them to move the conversation to another platform or asks them to keep a conversation secret). Let your child know they can come to you if something feels uncomfortable or someone alarms them, and that you'll listen and help.

Maintaining an open, non-judgmental conversation with your child can help ensure they can talk to you without shame.

Microsoft has a zero-tolerance approach to grooming behaviors across all our services and any discovered behavior should be reported to the platform. If you think a young person's safety is at risk, call local law enforcement.

LEARN MORE

Advice for teens: Gurls Out Loud

Advice for parents: TALK Checklist by the Internet Watch Foundation

What is Grooming? - Thorn for Parents

4. Sextortion

Young people may also be targeted for financial "sextortion" where a bad actor threatens to release nude or embarrassing imagery unless a payment is made. In many cases, this may arise where a young person believes they have been communicating with someone their own age who is interested in a relationship. This may prompt similar behaviors as grooming, or unexpected asks for money or cash equivalents such as gift cards. As above, because of the shame a young person may feel, it's important to have open discussions about online safety.

If someone threatens to share a nude image or video of someone (whether real or AI-generated), that is a type of image-based abuse and should be reported to the platform and to law enforcement or other local authorities. And if a teen has shared nude imagery or video taken when they were under 18 and is concerned it may be shared online, visit Take It Down for help to get them removed from participating online services.

LEARN MORE

Sextortion: What Kids and Caregivers Need to Know — FBIAdvice

Take It Down (ncmec.org)

Online Family Safety Guidance

1. Start the conversation early and keep it going

At every age, take an interest in young people's digital lives and talk with them about how they like to spend time online, the apps they're using, and the games they're playing. With younger kids, go online together and take a close interest in what they're doing – building safety awareness and practices from a young age will help establish good patterns for life.

As teens move over the age of 13, transition from reviewing their online habits to a more trust-based approach. Be supportive and positive, not judgmental, so they're more likely to come to you if something is worrying them.

HOW CAN OUR FAMILY SAFETY OR OTHER TOOLS HELP?

Use activity summaries or search history as a conversation starter – with younger kids, you may wish to have frequent conversations, as opposed to periodic check-ins as they get older. Talk about trends and any adjustments that may need to be made.

Leverage gaming to learn: Minecraft Education's module **CyberSafe: Home Sweet Hmm** aims to help teach ages 7-12 the basics.

2. Co-create boundaries with your child

Establishing clear boundaries is a critical part of digital parenting and leveraging parental control tools can help give you and your child confidence that they are safely navigating the online world. Discussing and agreeing on ground rules can help them feel empowered and a part of the decision-making process – kids are also more likely to stick to rules when they understand the rationale.

Setting boundaries might include who kids can contact or engage with online, screen time limits and the times of day and places where they can use a device, and discussions around the apps, games, and content they're permitted to access or purchase. Each family will have their own balance between supervision and supporting their child's online privacy and freedom.

HOW CAN OUR FAMILY SAFETY OR OTHER TOOLS HELP?

Use **app, game, and/or device screen time limits** to support a healthy balance between time offline and time online. When that runs out, you can choose whether to add more time, based on what's right for your family – you may choose to extend screen time for older children. For teens, this can be an open dialogue.

Use **content filters and SafeSearch** to help create a safe space to explore online and limit browsing their browsing in Microsoft Edge to child-friendly websites. For teens, talk about the kinds of sites and content they might want to avoid and how to report it if they are exposed to anything concerning.

Read the **Code of Conduct** in the **Microsoft Services Agreement**, and other Microsoft service-specific rules, so you're familiar with what is allowed on our services.

3. Learn about the apps and services your child is using

Get familiar with the apps, games and other online services your child frequents to identify potential issues or trends in their digital behavior. Visit the websites your child wants to visit, use the apps, and talk to them about downloading from reputable sources to avoid malware. Test the games they want to play and discuss any apps or in-app items that require purchasing. It's also important to be aware that many online services have age restrictions (e.g., some services do not permit children under age 13 to have accounts) or may offer child-specific accounts.

Evaluate the devices your child wants to use before they use them—preferably before you even buy them. Experiment to make sure you're comfortable with their features. Restrict any functionality your child isn't yet ready for.

For younger children, consider putting internet-connected game consoles and computers—especially those with webcams—in central family spaces and explain why you're doing this. Make video calls there, too. This helps you engage with and protect your child more comfortably.

HOW CAN OUR FAMILY SAFETY OR OTHER TOOLS HELP?

Set up and manage child accounts so you can use the parent controls correctly. **Adding people to your family group** allows you to manage limits and permissions, and view activity reporting details.

Use classifications and app store ratings through the **Microsoft Store**.

Use **content filters** to establish internet boundaries to protect yourself and your family from inappropriate web content.

Set age limits to prevent apps and games on Microsoft and Xbox Store from being downloaded or run if already installed. Or set filters to block specific apps and games on Windows, Xbox, and Android.

4. Protect your security and data

Explain to your child what "personal information" means and teach them to keep it private. Depending on age and maturity level of your child, you will be the ultimate judge of how to explain this. It's also important to stress the value of personal information to those who may want to exploit it—bullies, predators, and identity thieves. Speak with your child about asking you if they should share personal information about themselves, friends, or family in texts, email, or on social sites.

Help your child create email addresses, screen names, and gamer tags that don't reveal anything personal, or suggestive, and don't make them easy to locate.

Help your child create strong passwords, mixing capital and lowercase letters, numbers, and symbols. It's also important to emphasize that your child should not share passwords with anyone but parents or a trusted adult—not even best friends.

Teens will be reminded of the cybersecurity basics in school, but it never hurts to remind the whole family to think before they click and to be wary of any email that looks to good to be true.

HOW CAN OUR FAMILY SAFETY OR OTHER TOOLS HELP?

Cybersafe: Home Sweet Hmm provides a fun way for your child to understand how to identify and avoid common cybersecurity risks by remembering, "STOP and THINK before you CLICK".

Microsoft Defender Smartscreen helps you stay protected while you browse the Internet by blocking phishing and malware attacks. **Password Monitor** can check your saved passwords against data breaches and send you an alert if a password is unsafe so that you can change it immediately.

Protect your home network with encryption such as Wi-Fi Protected Access (WPA) and only use other people's networks for sensitive or personal tasks if they're also secured.

5. Be privacy aware

For users under the age of 13 or as specified by law in their jurisdiction, certain Microsoft products and services will either block users under that age or will ask them to obtain consent or authorization from a parent or guardian before they can use it, including when creating an account to access Microsoft services. We will not knowingly ask children under age 13 to provide more data than is required.

Note that each online platform and app come with its privacy approaches to their customer's data. It's important that you understand how your data is used and how to adjust privacy settings on the platforms you use. Certain privacy settings allow you to control who sees your child's information and activities. You can learn more about these settings on our services and Microsoft Family Safety in the product-specific section in the **Microsoft Privacy Statement**.

HOW CAN OUR FAMILY SAFETY OR OTHER TOOLS HELP?

At Microsoft, we believe privacy starts with putting you in control of your data. Your **privacy dashboard** is the place where you can view and clear data that Microsoft saves to the cloud. This data includes your browsing and Bing search history, location data, apps and services activity, and more.

Make learning a game, with strategies for protecting personal data utilizing areas of trust and safety available in Minecraft's **Privacy Prodigy**.

The **Privacy for young people** webpage is a great resource for parents and young people to learn more about Microsoft's privacy practices, and how to use our products in a way that protects your privacy.

6. Model empathy and digital civility

As your child's online experience grows, it's important to encourage them to display respectful and empathic communication and behavior. Remind them that if it's not OK to say or do something face to face, it's not OK online. Showing more kindness, empathy, and respect in our everyday encounters ensures that online interactions have a constructive impact on everyone involved.

Fostering a culture of digital civility is crucial for creating a positive and safe online environment. It helps prevent online abuse, encourages responsible digital citizenship, and supports the development of healthy and inclusive digital communities. As you and your child practice digital civility, you contribute to a more enjoyable, respectful, and constructive digital space for everyone.

HOW CAN OUR FAMILY SAFETY OR OTHER TOOLS HELP?

Find out what it takes to create peace through gaming in **Minecraft's Peace Builders**.

Take Microsoft's **Digital civility challenge** as a family.

Read the **Code of Conduct** in the **Microsoft Services Agreement** and any other service-specific rules so you're familiar with what is allowed on our services.

Talk to your child about reporting inappropriate content with **report a concern** and **how to use settings** and preference tools to block content.

7. Encourage your family to ask questions

As young people go online, it's important to support dialogue about the material they may encounter online and to understand some content may be designed to misinform, whether intentionally or otherwise. Misinformation is where false information is shared by accident, whereas disinformation is false information that is shared deliberately, including to mislead and cause harm.

Early on, encourage your child to ask questions about what they see or read and to develop critical-thinking skills to judge the accuracy and objectivity of online information. Have conversations with them about distinguishing fact from opinion and how to recognize bias, propaganda, and stereotyping. Talk to teens about research and using a range of sources. This is also important in an age of generative AI technologies – the very next topic in this guide!

HOW CAN OUR FAMILY SAFETY OR OTHER TOOLS HELP?

Learn some media literacy tips through gaming with the **InvestiGators from Minecraft Education**.

Tools like **Newsguard** can help provide more information about the sites you visit.

Navigating the Era of Artificial Intelligence

What is artificial intelligence?

Artificial intelligence (AI) is a field of computer science and technology that focuses on creating machines, software, or systems that can perform tasks that in the past have typically required human intelligence. These tasks include things like understanding language, recognizing patterns, and making decisions.

We've become accustomed to using AI at home, work, and play – from digital voice assistants, algorithmic feeds that personalize our news and entertainment, smart home appliances, wearable health devices, learning platforms, videogame enemies, and productivity tools. But in the last 12 months, we've seen the emergence of new "generative AI" tools and services.

What is generative AI?

Generative AI refers to a type of AI that is designed to generate new content or data. It uses machine learning models to produce original content, such as text, images, music, or even videos, some of which may be indistinguishable from content created by humans. Generative AI systems are based on sophisticated large language models (LLMs), which are trained on very large amounts of text data, enabling them to predict what word should come next in a sequence. LLMs are capable of performing a variety of tasks, such as text generation, summarization, translation, classification, and more.

However, LLMs also come with challenges and risks. LLMs are trained on large datasets and if datasets contain biased information, for example, the model can perpetuate and even amplify these biases. This can result in unfair or discriminatory responses. AI is an incredible technology, but like any technology, it's important to understand how it works and some of the potential challenges.

Our approach to responsible AI and child safety

We take our commitment to responsible AI seriously. **Microsoft's AI principles** and **Responsible AI Standard** are focused on proactively establishing guardrails for AI systems so that we can make sure that their risks are anticipated and mitigated, and their benefits are maximized. This has included assessing potential risks for young users and developing mitigations to address them.

From our longstanding efforts to advance digital safety, we know that young users have unique needs. And research shows that adolescents experience technology differently than adults, meaning AI may create different opportunities and risks for young people.

When it comes to generative AI services, Microsoft recognizes there is a valid concern that young users may not always understand the limits of the technology that they are engaging with, particularly when that technology is relatively new. For example, with conversational or "chat" AI features, young people may be inclined to provide more personal information than they would to a search engine. Young people also might be tempted to use these features in inappropriate ways, such as to cheat on homework.

Tips for Parents

We've released some guidance for educators through **TeachAI** and to support classroom discussions on AI with the **"Unlock generative AI safely and responsibly – classroom toolkit"**. But parents and caregivers also have an important role to play in helping young people understand the technology. We offer some suggestions below and you may wish to check out other resources, such as the Family Online Safety Institute's **GenAI Conversation Starters**.

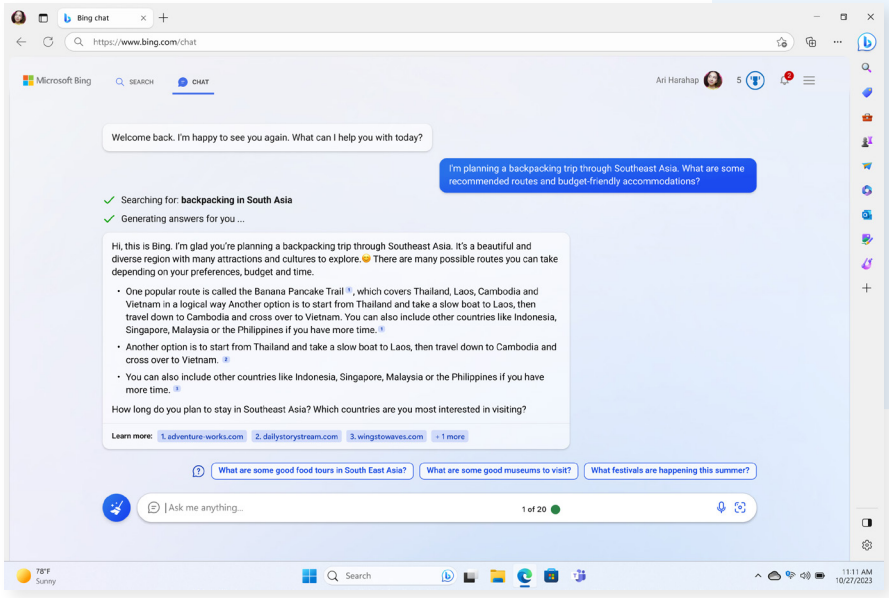
Help young people understand what the technology is and what it is not:

Because AI models and chatbots can respond conversationally, it's important to help young people remember that this is still an AI model. AI cannot replace real human connections or conversations – remind young people to set healthy boundaries.

HOW CAN WE HELP?

The Copilot interface includes disclaimers that make it clear to the user that they are engaging with an AI product and link to further information about how it works.

Consider whether your child could use Copilot's balanced or precise modes, versus creative mode, which will result in more creative or elaborate responses.



Support your child to use AI as a co-pilot:

AI models can sound very convincing, but they can produce biased, misleading, or not well-supported responses. We've taken a range of steps to reduce these risks but it's helpful to remind young people that mistakes are possible, so they should use AI as a co-pilot to support their own work and thinking. Encourage them to use their judgment and to test any responses they get from AI chatbots or services.

HOW CAN WE HELP?

Because Copilot leverages Bing search, the answers include links showing where it obtained information to support that answer. You can review these sources together and use them to find additional information.

Copilot provides tools for quick feedback: if a response is inaccurate or makes a young person uncomfortable, hit the thumbs down or report the content to us.

Increasingly, images and videos generated by AI will include source information that helps explain where they came from. With older teens, explore using online tools to test content sources.

Remind young people not to share personal information:

Data collection in Copilot is used only to provide the service and contextually relevant ads (note that we do not target ads to users under the age of 18). However, as with every online service, remind your child to never share personally identifiable information, whether it's about them or someone else. This means safeguarding information like their full name, email address, phone number, home address and other sensitive data.

HOW CAN WE HELP?

Encourage young people to review the Microsoft Privacy Statement and terms of service for an AI tool before using it – this will help them understand how their data will be handled.

Leverage Safe Search and parental controls:

When signed into Copilot using a Microsoft account, you can enable Microsoft's family safety settings, including activity reporting and allowing parents to control the level of Safe Search protection for their children in both search and chat.

HOW CAN WE HELP?

Your family's network administrator can also **choose to disable chat entirely**.

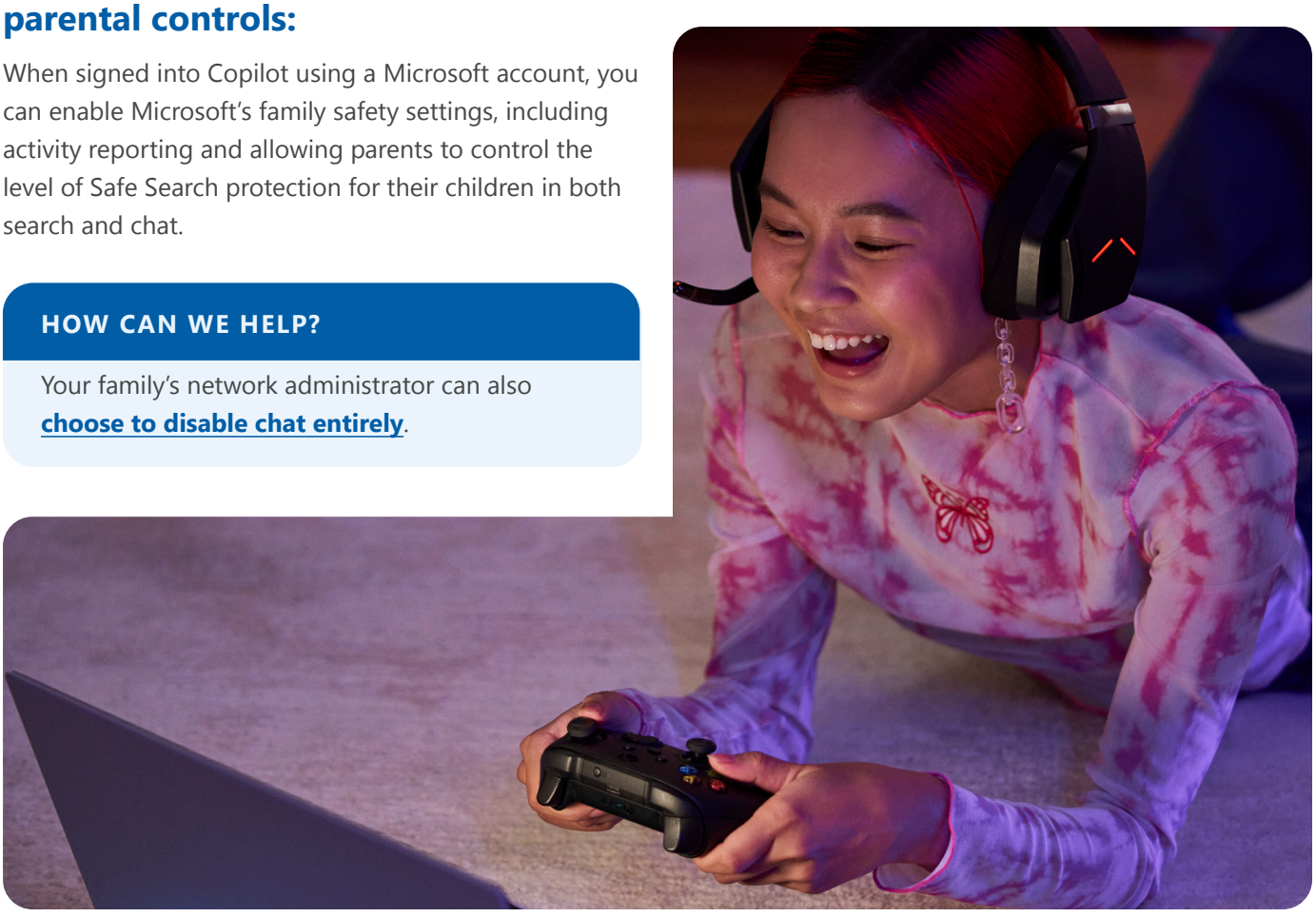
Encourage good digital citizenship:

As with any other technology, it's important to use it responsibly and wisely. That includes following any classroom or other school rules about the use of AI in homework and avoiding using the technology to generate any content that could cause harm to others. For instance, talk about the potential consequences of misusing another person's image to make an embarrassing picture using AI.

HOW CAN WE HELP?

Take the time to review the terms of use for Copilot and understand the rules that apply to the service – for younger users, consider reviewing them together and discussing the ways in which generated content could be used for good.

Consider taking the **Digital Civility Challenge** as a family.



Up your prompt engineering game:

Work together as a family to make the most of your AI-powered assistant in search! Share tips and tricks as a family, such as:

Ask questions that are as detailed and concise as possible.

Avoid using relative terms, like *yesterday* or *tomorrow*, and pronouns, like *it* and *they*. Instead, use specifics, such as an exact date (like November 19, 1863) or a person's name (like Abraham Lincoln).

Keep giving us your feedback!

Feedback about your experiences with Copilot can be logged using the following tools:

Through the blue "feedback" button at the bottom right of your results page and the bottom of the Microsoft Edge sidebar.

Throughout the Bing experience you will notice thumbs up/ thumbs down buttons you can interact with to log feedback.

At bing.com/chat you can click on the "Let's learn together" square.