Online Safety Newsletter

Nov 2026

Spotify Parental Controls

Spotify is a music streaming service. You must be aged over 13 to access it. If under 18, parent/guardian consent is required. However, under-13s can access Spotify through a **managed account** set up by a parent or legal guardian.

Since July 2026, Spotify has provided parental controls for managed accounts on both free and premium plans. These controls:

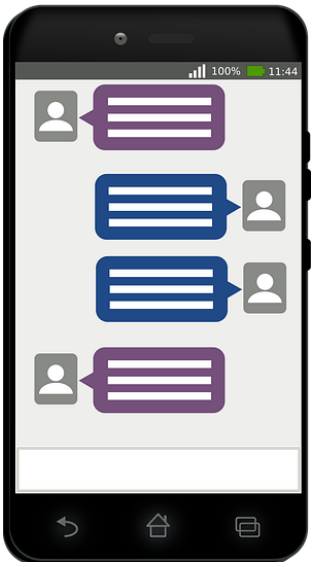
- turn messaging off.
- turn explicit content off.
- turn videos and canvas off.
- allow you to block specific artists or tracks.

Further information

Read the news announcement here: https://newsroom.spotify.com/2026-05-13/managed-accounts-free-tier-expansion/

Spotify have produced this Parental Guide to assist you with further information: https://www.spotify.com/us/safetyandprivacy/parental-guide

Online Grooming



What is Online Grooming?

Online Grooming is when an adult builds a relationship online with a child to manipulate, exploit, or abuse them.

How does Grooming take place?

Groomers often use fake profiles to pretend they are someone they are not, for example they may claim to be younger than they really are or pretend to be a person of influence. They will use flattery and attention to build trust and friendship. They may use online games or social media to initiate contact but then encourage your child to switch to a different app to chat with privately - usually on an app that offers limited or no parental controls and/or encrypts messages.

What can I do?

- Use appropriate parental controls.
- Set privacy settings.
- Show them how to use any blocking or reporting tools.
- Chat to your child regularly about what they do online and who they communicate with. Remind them that people online may not always be who they say they are.

What are the signs that my child is being groomed?

- Being **secretive** about who they are talking to.
- They become **withdrawn** from family and friends.
- Appearing **anxious or upset** after receiving messages.
- Receiving unexpected **gifts**.

Find out more here: https://learning.nspcc.org.uk/safeguarding-child-protection/offender-gaining-trust

What should I do if my child is being groomed?

- If you think your child is in immediate danger, contact the police.
- Stay calm and reassure your child that they are not to blame.
- If you are worried about online abuse or the way somebody has been communicating with your child online, report it to CEOP: (https://www.ceop.police.uk).

Further information

- https://www.ceopeducation.co.uk/11_18/lets-talk-about/sexual-abuse/online-grooming/

COM Networks

COM Networks are online communities where harmful and deeply disturbing behaviour occurs, including child sexual abuse, cybercrime and extremism. These networks operate on mainstream messaging apps, gaming platforms and through social media. **It is important to be aware that such networks exist and understand the risks they can pose to children.** Introductions to COM Networks can begin with harmless conversations on a game or social media platform, but then as trust builds, groups will gradually introduce harmful content, extreme challenges and pressure to prove loyalty. Some groups use threats, humiliation or the threat of exposing private information to control members. Images, messages or personal details may be used to blackmail victims.

What should I look out for?

- **Increased secrecy**
- **Emotional or behavioural changes**
- **Unfamiliar language:** using new expressions or discussing extreme content, opinions or beliefs.
- **Unexpected gifts**

Sky News investigation into COM Networks (and links on popular sites such as Roblox and Discord)

You may have seen Sky News' investigation into COM networks. The report highlights findings from a six-month investigation that found self-harm-themed avatars, clothing and related content available on the gaming platform Roblox, including items that could be **accessed by children as young as five years old**. The report can be viewed here, **please be aware that it contains upsetting content**:
https://news.sky.com/video/inside-robloxs-dark-side-sky-news-finds-self-harm-avatars-available-to-young-children-13592551

How can I protect my child?

- Have regular and open conversations with your child. Ask your child what they do online and who they communicate with.
- Reassure them that they can always ask for help, even if they have shared something personal or broken a family rule.
- It is important to remember that threatening to confiscate their devices may make them less likely to talk to you when something goes wrong.
- Regularly review privacy settings and set up appropriate parental controls on all devices your child is using.
- Ensure your child understands the risks of sharing personal information or intimate images online.

Further information

- https://www.gloucestershire.gov.uk/gscp/professional-resources/sadistic-online-exploitation/
- https://saferschoolsni.co.uk/understanding-com-networks/

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date released 01.11.26. The inclusion of any links does not imply any affiliation with or endorsement of the linked websites, documents, or videos, nor are we claiming any ownership or copyright in the content of the linked materials.

WhatsApp Channels and Parental Controls

Users must be at least 13 years old to use WhatsApp. Children under 13 can access WhatsApp through **a parent-managed account.**

WhatsApp Channels

WhatsApp Channels are a one-way broadcast tool to send updates to followers. Channels can be found in the Updates tab. From here you can view a whole host of channels, including channels that will **not be age appropriate and may include adult content.** If your child has their own WhatsApp channel, then you need to be aware that they are **public. Anyone can view and follow a channel and anything you share on your channel is public.** We would recommend that parental controls are used to prevent children creating and accessing WhatsApp channels.

Parent Managed accounts

Parent managed accounts are required for those under 13. These accounts have additional safety restrictions and do not allow access to features such as Channels, Meta AI and location sharing. You also have control over which groups they can join.

Parental Controls for Teenagers

For users aged 13 to 17, WhatsApp offers parental control settings to limit access to certain features such as Channels.

For more information, visit:
https://www.whatsapp.com/parentalcontrols

Rage Bait

Have you heard of this term? Rage bait is when somebody deliberately posts online content to make people feel angry or frustrated to generate views and engagement. Find out more here: https://findmykids.org/blog/en/rage-baiting