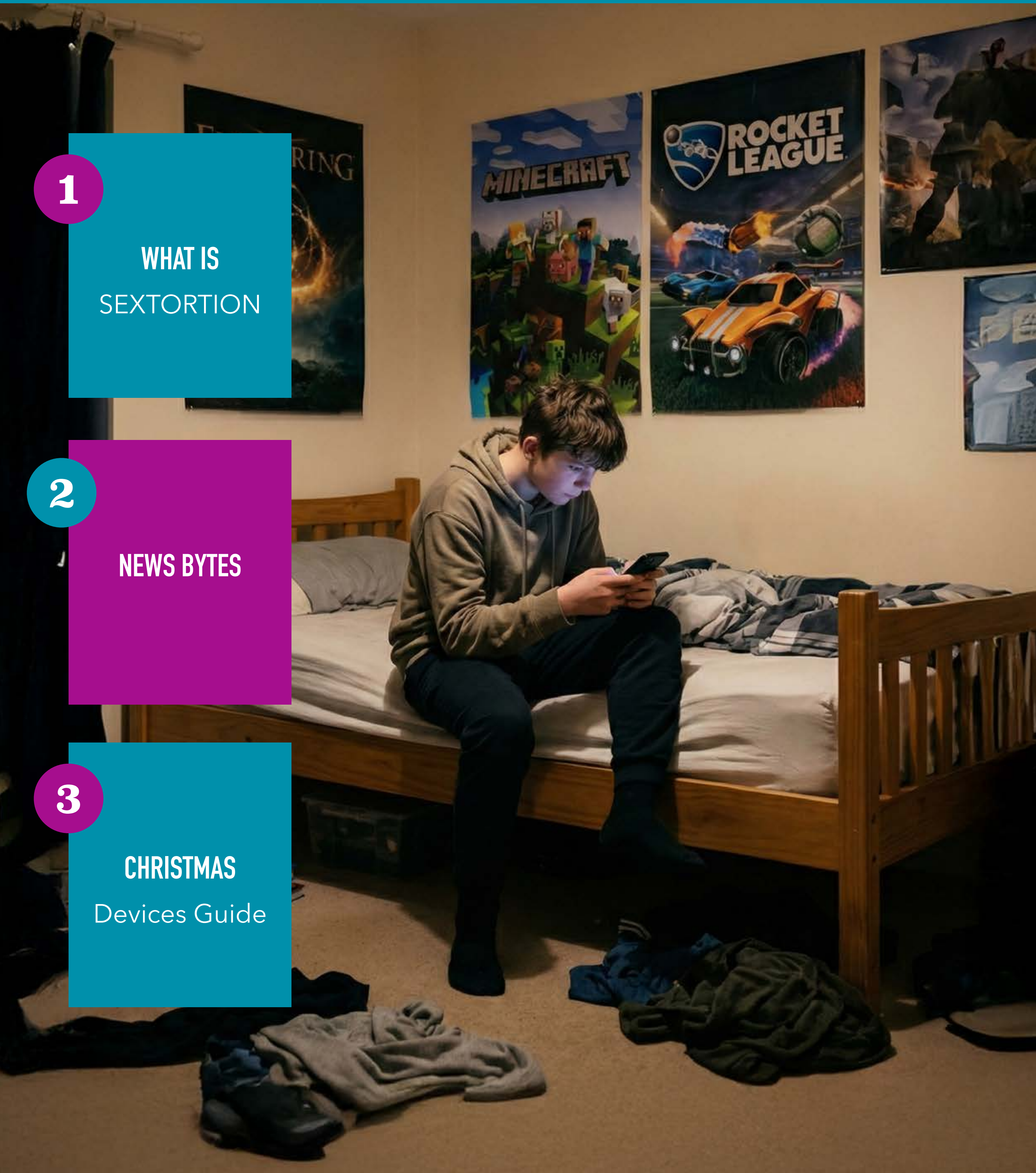
SAFE and SMART

Keeping Children Safe Online

December 2025



1 **WHAT IS** SEXTORTION

2 **NEWS BYTES**

3 **CHRISTMAS** Devices Guide

What is:
SEXTORTION?

Sextortion is a form of online blackmail
where an offender pressures a young person into sharing a nude or sexual image (or captures one during a chat or video call) and then threatens to share it unless the child does what they demand. The demand is often for money, gift cards, or more images. It frequently starts with what looks like a friendly, flirtatious conversation on social media, messaging apps or even gaming platforms, before turning into threats.

It can happen fast; a child might believe they're chatting to another person of similar age, only to discover the profile is fake. Once an offender has an image, or even a screenshot, they may show the child their social media follower list and claim they'll send the image to friends, family or school contacts unless payment is made. The urgency is deliberate: panic makes it harder for a child to think clearly or reach out for help.

Sextortion is being treated as a growing safeguarding concern around the world. For example in the UK The Internet Watch Foundation (IWF) reported that between 1 January and 30 June 2025 it confirmed 153 child sexual extortion reports, compared with 89 in the same period in 2024 — a 72% increase. The IWF also notes that boys made up 97% of confirmed cases in that period, though girls are also affected and may experience different forms of pressure.

Support services are also seeing this concern show up in real lives. Childline delivered over 900 counselling sessions about sextortion in 2023/24, and they handled over 150 contacts from adults concerned about it. Where gender was known, around 68% of these Childline sessions were with boys and 31% with girls. This pattern aligns with what schools are noticing too: many cases are financially motivated and target teenage boys (although younger children have also been targeted), but the emotional harm for any child can be profound.

It’s also worth knowing about the scale of image-related reporting. The IWF and Childline’s Report Remove service, which helps under-18s confidentially report and remove sexual images of themselves, received 1,142 reports in 2024, a 44% increase on 2023. The biggest rise by age group was among 11–13-year-olds, increasing from 13 reports in 2023 to 69 in 2024. The service also allows young people to report AI-generated or manipulated images that appear to be them.

If your child is ever targeted, the most important first step is reassurance. They need to hear clearly: **“You’re not in trouble. You’re not to blame. I’m here to help.”** Offenders rely on shame and fear to keep children silent. Try to stay calm, encourage your child not to pay (payment often leads to further demands), and help them save key evidence such as usernames, messages and screenshots to pass onto the Police. Report and block the account on the platform involved, and consider using Report Remove if an image of your child is involved (search: Childline Report Remove).

A simple preventative message can make a big difference: **if anyone asks for images or makes threats, screenshot and tell a trusted adult straight away.** Offenders will often delete images, chats and accounts quickly to prevent being caught.

Regular, low-pressure conversations about online relationships, fake profiles and what to do when something feels wrong are often more protective than a one-off “big talk.” Sextortion is designed to make children and young people feel trapped — but with prompt, compassionate support, they are not trapped.

Roblox

Roblox is about to tighten up who can chat with whom, and it's a change parents will welcome as Roblox plans to make facial age checks (or ID checks) mandatory for anyone who wants to use any chat features, with the rollout beginning in December 2025 in some countries and expanding more widely in early January 2026.

The idea is simple: instead of relying on a child's self-declared birthday, Roblox will use a quick age-check to place users into age bands such as Under 9, 9–12, 13–15, 16–17, 18–20, and 21+. Chat will then be limited mainly to people in the same or nearby age groups, which should reduce risky contact between children and adults. Roblox says that for children under 9, chat in games will be off by default unless a parent enables it after an age check.

Internet Safety Glossary

Are you CHEUGY? Do you know your AR from your ASMR? What about BLOATWARE and BUSSIN, or even GRIEFING?

Internet slang seems to constantly change, but Internet Matters have put a handy guide together. This could be a fun family game, seeing who knows or who can guess.

You can find the guide here: https://www.internetmatters.org/resources/glossary/

Android Parental Controls

Google have recently updated the Android operating system. There are a number of changes, including more parental controls which includes:

- Set the amount of screen time that can be spend on a device.
- Set downtime schedules to automatically block the device at night.
- Control app usage by limiting the time.
- Add more time by granting extra minutes.

There is a handy guide to setting up Android parental controls on the Internet Matters website here:

https://www.internetmatters.org/parental-controls/smartphones-and-other-devices/android-smartphone/

Holiday periods such as Christmas gives us a great opportunity to set healthy habits from day one. The good news is you don't need to be a tech expert to make a big difference. A few simple settings, plus clear family expectations, can help children enjoy their new phone, tablet, console, laptop or PC more safely.

A handy approach is to do a quiet "grown-up set-up" before the device is wrapped. Get familiar with the safety features, switch on age-appropriate settings, and think about where and when your child will use the device. For example, encouraging gaming and browsing in shared family spaces can make it easier to keep an eye on what's happening without hovering. Setting a daily time limit and having a clear evening cut-off helps protect sleep, and many families find it useful to keep devices out of bedrooms overnight.

It's also worth reminding children that people they meet online are still strangers, no matter how friendly they seem, and that they should come to you if anything feels odd or upsetting. One of the most important things to remember is a calm, ongoing conversation where your child knows they won't be blamed for speaking up. Playing games together or exploring apps with them can turn safety into something collaborative rather than a "rule book."

On the following page is a very simple but handy checklist of things for you to consider, but above all have fun and enjoy the experience with your child.

If you need help setting up devices, Internet Matters has a great resource page here:

https://www.internetmatters.org/parental-controls/

PARENT’S CHECKLIST:

1) Home internet first

☑ Turn on parental controls on your broadband (filters, age ratings, time limits).

2) If it’s a smartphone

☑ Set mobile network controls as well as device controls.

☑ Review privacy, location and contact settings.

3) Set up the device before gifting

☑ Create a child account (not an adult one).

☑ Use device-level restrictions for age-appropriate apps, content and purchases.

☑ Disable or restrict location services.

☑ Turn on password/biometric locks.

☑ Set in-app purchase protections to avoid surprise bills.

4) If it’s a games console (Xbox/PlayStation/Nintendo)

☑ Set the child’s profile age correctly.

☑ Turn on console family/parental controls:

- ☑ age ratings for games,
- ☑ spending limits,
- ☑ communication settings
- ☑ screen-time limits.

5) If it’s a laptop/PC/tablet

☑ Use a child user profile.

☑ Enable safe search and age filters.

☑ Check app stores are locked to age-appropriate downloads.

6) Family rules that really help

☑ Agree where devices are used (shared spaces works well).

☑ Set a simple holiday screen routine (more flexible is fine, but still with boundaries).

☑ Have a ‘come to me early’ promise if something goes wrong.

Common Apps

This is not an exhaustive list, but tends to be the more popular apps used by children and young people.

Age requirements are set within the terms and conditions of the app provider, don't be confused by ratings in the app stores which can be

App	Age	Comments
	13	**Discord** - is a voice, video and text chat app that's used by tens of millions of people aged 13+ to tap and hang out with communities or their friends. Parental settings can be found **HERE**.
	13	**Instagram** - is a photo and video sharing app where people can upload photos, videos and messages to share with others. Parental settings can be found **HERE**.
	13	**Snapchat** - is a very popular app that lets users swop pictures and videos (Snaps) with others which are meant to disappear after they are viewed. There is also a messaging feature. Parental settings can be found **HERE**.
	13	**TikTok** - is a social media app that allows users to create, watch and share short videos shot on mobile devices or webcams. Parental settings can be found **HERE**.
	13	**Twitch -** is where people come together to chat and interact live. Think YouTube, but it is live rather then pre-recorded. Parental settings can be found **HERE**.
	13	**WhatsApp -** is a messaging app which uses text, images, video and voice record features to connect with others. Parental settings can be found **HERE**
reddit	18	**Reddit** - is a network of communities (called subreddits) where people can share information, their interests and hobbies. Reddit is an 18+ app, there are no parental controls.