

A PARENT'S GUIDE



Safe Play.

Child safety in Android games
and what's really going on inside
kids' games



Brought to you by **Pumpkin Cat Games**

By the end of this guide, you'll...

Know

- How “free” games really make their money
- What each “Allow” hands over, and which requests are red flags
- What an age rating tells you, and what it can't

Have set up

- ✓ Your approval on every download and purchase
- ✓ Chat switched off, or limited to friends
- ✓ A private profile and a daily time limit

Be ready for

- The warning signs worth acting on
- Who to call, and how to get your money back
- The conversations that keep your child coming to you

It won't make games risk-free.

It will mean you're **no longer guessing.**

Short on time? Start with the checklist on page 33.

no tech degree required

Settings menus change as apps update. If a screen looks different on your device, search its settings for the feature by name.



Inside.

Part 1 **Getting your bearings**

- 01** Introduction 4
- 02** Android's built-in controls 6
- 03** Permissions and data 8

Part 2 **The hidden costs**

- 04** In-app purchases 10
- 05** Chat and strangers 12
- 06** Ads and dark patterns 14

Part 3 **Healthy habits**

- 07** Age-appropriate games 17
- 08** Screen time 19
- 09** Privacy and accounts 21

Part 4 **When it matters**

- 10** Red flags 23
- 11** If something goes wrong 25
- 12** Ongoing conversations 27

Part 5 **A better way**

- 13** Why safe gaming needs better games 29
- 14** A note from the author 31

Extras **Appendix and sources**

- A** Quick-reference checklist 33
- S** Sources 36

01

Introduction.



Chances are, if your child has an Android phone or tablet, games are one of the main things they use it for.

This isn't a small thing any more. It's worth pausing on just how big a part of daily life gaming has become for children — and how much has changed about what games actually do.

Modern mobile games aren't just entertainment. Many are built around collecting personal data, showing ads, and encouraging spending — sometimes before a child even understands what they're agreeing to.

97%

of 8–17-year-olds play online games¹

53%

of those players spend money inside the games¹

“Just as tellingly, a third of children who spend money online regret their in-game purchases^{1,2}”

Then there’s the social side. Many popular games now include chat, voice calls, or open multiplayer lobbies — features that let your child talk to people they’ve never met.

22%

of 8–17s talked while gaming to people they didn’t know outside the game (2023)³

31%

of 8–17s who game online chat with strangers while gaming (2024)⁴



None of this means gaming is bad for kids. It means the landscape has shifted, and the tools and habits that kept children safe a few years ago might not be enough today.

This guide walks through what’s actually going on inside these games, and what you can do about it — without needing to become a tech expert first.

let’s begin.

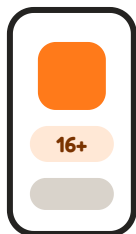


02

Android's built-in controls.

Before you download a single game safety app or spend money on extra software, it's worth knowing that Android already comes with a decent set of tools – most of them free, and built by Google itself.

The main one is Google Family Link. Once you've linked your child's account to yours, you can make every new app they try to download from the Play Store wait for your approval before it installs^{5,9}. So if your eight-year-old tries to grab a game rated for 16+, it won't go through without you saying yes first.



may I?



Rated 16+ for an eight-year-old? It won't install without your yes.

What Family Link lets you control

- ✓ **Approves downloads and purchases**
For every install, or only paid apps and in-app purchases⁹
- ✓ **Caps content by age rating**
Set a top rating for apps and games, films and TV, though higher-rated titles may still show in search⁶
- ✓ **Blocks apps and sets time limits**
Block any app outright, or cap daily use^{5,7}
- ✓ **Keeps the controls with you**
For a supervised child, restrictions are changed from your account, not theirs⁶

It's worth being honest about the limits

- ! Family Link's content filters work mainly across Google services like Play, Search, Chrome and YouTube^{6,8}.
- ! Family Link can't filter chat inside a game, and its website filters only reach Chrome and some apps.

13

At 13, your child can move to a supervised teen account. Until they're 18, they need your approval to stop supervision⁸

Think of this chapter as your
starting point, not your whole toolkit.



03

Permissions and data.

When a new game asks to access your camera, microphone, contacts, or location, it's easy to just tap “Allow” and move on. But each of these permissions means something specific – something worth knowing before you agree.



Camera

Lets the app take photos or record video through the camera



Microphone

Lets the app record sound, from your child's voice to whatever's nearby



Contacts

Lets the app read everyone in your child's address book, not just other players



Location

Lets the app see where your child is and, with “Allow all the time” set, keep tracking in the background¹⁰

does this permission match
what the game actually does?



Makes sense

- ✓ **A game with voice chat**
needs the microphone
- ✓ **A “scan to add a friend” feature**
needs the camera

Red flag

- ! **A simple puzzle or colouring game**
asking for your contacts or location is a warning sign, not a formality

What the research found

Not every request is justified. A 2018 University of Michigan review of 135 apps used by children aged five and under found that 11 asked for microphone access, 9 for the camera and 6 for location. Some had legitimate gameplay uses, but the researchers said collecting a young child’s location raised concerns under US children’s privacy law¹².

Check what’s been accessed

- 1 See which apps used your permissions**
On Android 12 and up: Settings → Privacy (or Security & privacy) → Privacy dashboard¹¹
- 2 Revoke anything that doesn’t add up**
Pick a permission, tap the app, and change its access¹⁰



04

In-app purchases.

Free to download doesn't mean free to play. Most games make their money once your child is already inside – through skins, loot boxes, power-ups, or virtual currency that makes real money feel less real.

Free to
download



Skins · loot boxes ·
power-ups



Real money feels
less real



Pay-to-win

Nudges children to spend by making free progress painfully slow, while a small payment removes the friction instantly



Loot boxes

Take it further — paying for a random reward, styled just like a prize draw, which is why Belgium treats paid loot boxes as illegal gambling

Both are designed to take advantage of impulse control that's still developing.

\$245M

FTC settlement with Epic Games, maker of Fortnite. The FTC alleged its “counterintuitive, inconsistent, and confusing” buttons led players into unwanted purchases¹³

Surprise charges are a real, well-documented problem — not a rare mishap. In Fortnite, the FTC said, children could rack up unauthorised charges without any parental involvement¹³. The settlement bars Epic from charging players without their affirmative consent¹⁵, and Epic separately added a “hold to purchase” confirmation¹⁴.

Lock it down on Android

1 Require purchase approval

Use Family Link to require approval for every transaction

2 Add a check at the till

Play Store → Payments and subscriptions → Purchase verification: choose Always, and keep biometrics off if your child’s fingerprint is on the device¹⁶

3 Remove saved card details

Take them off your child’s device where you can



Check your Google Play purchase history occasionally

Small, repeated charges are easy to miss until they add up



05

Chat and strangers.

Many popular children's games now come with some way to talk to other players – text chat, voice chat, friend requests, or open lobbies where anyone can join.

Text chat

Voice chat

Friend requests

Open lobbies

These features are often switched on by default, before a parent ever gets the chance to say no.

31%

This isn't a hypothetical risk. Ofcom found that 31% of 8–17-year-olds who game online chat with strangers while gaming⁴

friends

strangers?

Two cases worth knowing



Fortnite, 2022

An FTC settlement required Epic Games to switch voice and text chat off by default for children and teens. The FTC alleged chat had been on automatically, exposing young players to bullying and harassment¹⁵



Roblox, 2025

An investigation by ITV News and the Global Project Against Hate and Extremism found extremist content circulating on Roblox, a platform used by children as young as seven¹⁷

To reduce the risk



Turn chat off, or limit it to “friends only”

Most games let you do this in the settings menu — do it before your child starts playing, not after



Use Family Link for the bigger picture

It can't switch off chat inside a game, but you can approve each install, block an app entirely, and set time limits⁵



Agree one simple rule with your child: if a stranger asks to move the conversation to another app, that's always a no, and always worth telling you about.



06

Ads and dark patterns.

This is where “free” games show their real cost — someone always pays, one way or another.

The Fortnite case is the one to know. In 2022, the FTC took action against Epic Games over what it called “dark patterns” — design tricks it said led players into unwanted purchases¹⁵.

Screen 1



Circle = cancel

Screen 2



Circle = confirm

The same button could cancel on one screen and confirm a purchase on the next — so a child who’d just learned “circle cancels” would find “circle confirms” moments later¹⁸.

same button, opposite meaning



Preview next to buy

The FTC alleged Epic put the button to preview an item very close to the button to buy it, so one misplaced tap could buy it¹⁹



Charged while loading

Players reported being charged while the game was loading, or waking up from sleep mode¹⁹

\$245M

to fund refunds for players²⁰

\$275M

further penalty over alleged child privacy violations — at the time, the largest for breaking an FTC rule²⁰

Data-driven ad targeting is just as concerning

New Mexico's Attorney General sued a children's game developer, alleging its apps used ad software from AdMob, InMobi, AppLovin and others to track children for personalised ads, in breach of US child privacy law²¹.

And then there's the consent screen problem

Consent screens can list hundreds of advertising partners, each with its own toggle — and often put “Accept” on the first screen with no equally easy “Reject all”²².

Your privacy choices

Advertising partner 1 ☒

Advertising partner 2 ☒

...and hundreds more

Accept all

The ad industry's main consent framework, IAB Europe's TCF, has hundreds of registered ad-tech vendors, any of which a single banner could list²³.

(an illustration)

Here's the uncomfortable part: research suggests few people read them, adults included.

90%

of young adults in one small study accepted or closed the banner just to carry on; none read it²⁴

1 in 10

US consumers say they always understand cookie notices; over half accept without understanding²⁵

Little research looks at children and these banners — but child-privacy experts point out a more basic issue: the frameworks make no provision for parental consent, even on children's sites where no parent is likely to be present²⁶. If adults skip past them, a child reaching for the "Play" button underneath almost certainly does too.

These aren't edge cases or rare bad actors. Fortnite, one of the world's biggest games, was penalised only after, the FTC says, millions of players had been tricked into unwanted purchases¹⁵. Confusing buttons, mismatched confirm/cancel actions and consent screens built to be skipped are design choices, not accidents — which is exactly why they're worth teaching your child, and yourself, to spot.



07

Age-appropriate games.

Ratings aren't just a suggestion – they're a genuine tool, and worth taking seriously.

On Google Play in the UK, most listings show a **PEGI age rating** (3, 7, 12, 16, or 18) under the title²⁷.



PEGI 7

Mild violence

Users interact, In-game purchases
(includes random items)

[Learn more](#)



the official PEGI labels

Using ratings on Google Play

1

Check before you install

The rating sits just under the game's title²⁷

2

Open it for the detail

Shows why it earned the rating, and flags features like chat²⁷

A rating reflects what's in a game, not how hard it is. **Content descriptors** — such as Violence, Bad Language, Fear or Gambling — show why the game earned its rating²⁸.



PEGI 12

Moderate violence

“**Moderate violence**” sits a step above the “Mild violence” on the PEGI 7 listing. Same layout, different story.



Parental guidance

Parental guidance recommended

Some listings say “**Parental guidance**” instead of an age number. Treat it as a cue to look closer yourself.

In North and South America you'll see **ESRB** ratings instead (E, E10+, T, M, AO), which work on a similar principle²⁷. You can also **cap the rating in Family Link**⁶.

A rating is only part of the story



Ratings come from developers' own answers

They fill in a questionnaire when they publish, and ratings can change after review³⁰



What a rating can't capture

How well chat is moderated, or how hard a game is to put down. Ratings don't cover features like chat²⁷, so independent parent reviews help fill the gap

79%

of parents whose children play video games know the PEGI labels; 62% of those use a tool to limit play (2023, UK and three EU countries)²⁹.



08

Screen time.

Gaming itself isn't the enemy — most children play without any issue. But it's worth knowing how modern games are actually designed to keep them playing, and what to watch for when that tips into something less healthy.

Recent UK figures put the scale of this in perspective:

nearly

1 in 3

11–16-year-olds report playing online games for four or more hours a day, often stretching late into the night³¹

9%

of UK adolescents, by one estimate, show symptoms consistent with “gaming disorder” — impaired control over play, prioritising gaming above other interests, and continuing to play despite it causing problems³¹

52%

rise in children's screen time between 2020 and 2022, with nearly a quarter using their phones in a way consistent with behavioural addiction³²

“None of this is an accident.”

Many games use reward loops, loot boxes and random prizes — the same kinds of mechanics found in gambling — to keep a child playing well past the point they intended to stop³¹.

Signs worth watching for

-  **Irritability or distress**
when asked to stop playing
-  **A drop in interest**
in things they used to enjoy
-  **Disrupted sleep**
-  **Play that continues**
despite clear negative consequences at school or home

Practical steps

-  **Set time limits**
In Family Link, or in the game itself if it has them
-  **Agree screen-free windows**
Meals and bedtime — a house rule, not a punishment
-  **Keep talking**
About how a game makes them feel, not just how long they play



09

Privacy and accounts.

By default, many gaming platforms are built to be public and social – which is great for connecting players, but not always great for privacy. Profiles, activity, and even real names can be visible to strangers unless you go in and change the settings yourself.

Public by default

Real name	visible
Location	shared
Profile	public

Left unchanged

After five minutes

Real name	hidden
Location	off
Profile	private

Adjusting settings

\$275M

civil penalty paid by Epic Games in its 2022 FTC settlement, over allegations it collected under-13s' personal data without parental consent. The FTC also alleged that on-by-default text and voice chat put children and teens at risk^{15,33}

“Default public” is often the easiest setting for a platform to ship, not the safest one for a child. A few practical steps make a real difference:



Set up a child account linked to yours

Google, Roblox, PlayStation and Xbox all let you link a child's account to your own, with age-based restrictions, and approve purchases, games or other requests from your account^{5,35–37}



Check privacy settings on every platform, not just the game

Use privacy settings so your child's details aren't visible to other players³⁴ — for example a private profile, no real name, and location sharing and personalised ads off



Use strong, unique passwords — and turn on 2-step verification

Turn it on wherever it's available — it helps stop someone hacking into your child's account³⁴



Limit who can send friend requests or messages

To friends only, or off, where the game allows it, so strangers can't contact your child directly^{35,36}



None of this needs to be complicated — most of it is a **five-minute job** in the settings menu, done once, that quietly protects your child every time they play afterwards.



10

Red flags.

Most of the time, a change in how your child plays is nothing more than a phase. But a cluster of changes — often around the time a new online contact enters the picture — is worth taking seriously rather than explaining away³⁸.

Behavioural signs to watch for

- ! Being secretive about chats, switching screens or apps when you walk in, or refusing to say who a “friend” from the game actually is
- ! Sudden mood swings tied to messages — a noticeable high when a notification arrives, followed by anxiety or low mood when it stops³⁸
- ! Becoming protective of their device — taking it everywhere, reacting sharply if someone glances at the screen³⁸
- ! Withdrawing from things they used to enjoy, or a marked change in sleep and appetite
- ! New arguments specifically about screen time, privacy, or “trust”

Technical and financial signs to watch for

- ! Unexplained in-game currency, gift cards, or credit**
appearing on their account — a well-known grooming warning sign, as groomers often use gifts to build a sense of obligation³⁸
- ! A new device or accessory you didn't buy them**
often explained away as “a friend gave it to me”³⁹
- ! Deleted message histories**
or an inability to describe who a contact actually is beyond “someone from the game”³⁹

7,263

online grooming offences recorded by UK police in a year, almost double 2017/18 where comparable. Where the platform was known, 40% were on Snapchat⁴⁰. Chats that start in a game can move to private apps, so watch where conversations go.



A single sign rarely means something is seriously wrong. But if several appear together, it's a reason to gently open a conversation, not to panic or confront — your child needs to feel able to keep talking to you, not shut down further.



11

If something goes wrong.

If something has already happened, the priority is simple: act calmly, act quickly, and keep your child talking to you.

999

If your child is in immediate danger, call 999 first⁴¹

0808 800 5000

NSPCC Helpline for adults, weekdays 10am–4pm. Children can call Childline free on 0800 1111, any time^{41,42}

If you suspect grooming or predatory contact



Report it to CEOP

The Child Exploitation and Online Protection Command, part of the National Crime Agency — ceop.police.uk/safety-centre. Children, parents and carers can report, and a Child Protection Advisor reviews it⁴¹



Know CEOP's remit

It covers sexual abuse and grooming only, not bullying, fake accounts or hacking⁴¹ — for those, the NSPCC Helpline or Childline are better first calls

If you're dealing with unauthorised spending

1 Find the purchase

Go to play.google.com, then Payments and subscriptions → Budget and order history⁴³

2 Request a refund

Click Report a problem on the order and ask for a refund, explaining what happened. Allow 1–4 days for a decision⁴³

Refunds like this aren't a favour. Google previously paid at least \$19 million in FTC-mandated refunds after children ran up charges without a password, or in a 30-minute window after one was entered⁴⁴.



If you need to uninstall a game

Remove it through Settings → Apps, not just by deleting the icon. Uninstalling doesn't cancel a subscription, so check Payments and subscriptions in the Play Store too

Talking to your child afterwards

“You're not in trouble, and I'm glad you told me.”

Lead with reassurance, not blame — it goes further than any question about what they did wrong. Many children delay telling a parent because they fear the reaction more than the incident itself⁴⁵, so how you respond in the first few minutes shapes whether they'll come to you again.



12

Ongoing conversations.

Everything in this guide so far — Family Link, content restrictions, purchase approval, privacy settings — genuinely helps. But none of it is a permanent fix, and it's worth being honest about that. **Technical controls have real limits.**



Children can and do bypass parental controls

A rapid evidence review by researchers at LSE and the University of Colorado Boulder found this, and little support for relying on parental controls as a stand-alone safety strategy⁴⁶



VPNs can get around network-level filters

About a quarter of 11–17-year-olds say they've used one, rising to almost a third by 16–17⁴⁷

76%

Even more telling: in a study of 736 reviews children wrote about parental control apps, 76% gave one star, many saying the apps felt invasive and hurt their relationship with their parents⁴⁸

Conversation

Family Link · restrictions · approvals · privacy settings

None of this means the controls aren't worth setting up — they are. It means they work best as a **foundation, not a substitute for conversation.**

Active mediation

European research led by LSE found that “enabling” mediation — talking about risks and helping children use the internet well, rather than just blocking it — goes with stronger digital skills and more opportunities (along with some more risk), while restriction alone cuts risks at the cost of those opportunities⁴⁹.

In practice, that might look like

- ✓ **Asking what a game is actually like**
genuinely curious rather than checking up
- ✓ **Talking through a red flag from Chapter 10**
before it happens, not just after
- ✓ **Being the one they tell about a weird message**
not the person they hide it from

Games and tricks will keep changing. A relationship where your child can come to you won't go out of date.



13

Why safe gaming needs better games.

Every chapter so far has been about vigilance — checking settings, reading permissions, watching for red flags, staying in conversation. All of it matters. But it's worth naming what this actually is: a defensive tax parents are paying, chapter after chapter, to compensate for a business model that wasn't built with children in mind.

Here's the scale of that model.

97%

of apps on Google Play are free to download⁵⁰

\$167bn

spent worldwide on in-app purchases and paid apps in 2025 (iOS and Google Play)⁵¹

\$82bn

of that went on in-app purchases in mobile games⁵¹

92.5%

of mobile game in-app purchase revenue in 2025 went to the top 1% of game publishers⁵³



A small minority drives the income

High-spending players, often called “whales”, drive a hugely disproportionate share of income while most spend little or nothing⁵²

“Put simply: ‘free’ was never really free.”

It means the game was built to make money some other way:



Ads

shown to a
captive
audience



Data

collected and
shared with third
parties



Purchase flows

engineered to
convert impulse into
spend

Every chapter in this guide, from reading permissions to spotting dark patterns to locking down purchases, exists because that’s the model the vast majority of children’s games are built on.

None of this is a criticism of any individual parent for not catching everything. The honest problem is structural — a handful of monetisation patterns, repeated across hundreds of thousands of titles, that parents are individually left to detect and defend against, game by game, setting by setting. Vigilance helps enormously. It was never supposed to be the whole solution.



The alternative isn’t more settings to configure.

It’s games built on a different foundation entirely — where the business model doesn’t need a child’s data, attention, or spending to survive in the first place.



14

A note from the author.

Everything in this guide so far has been grounded in research. This last chapter is different — it's personal.

I'm Drew, a dad of two from Surrey. This started the way it probably has for you: school homework moved onto an app, then music and language practice followed, and phones just became part of family life. That was the first wake-up call — in the modern app world, “free” rarely means free. It almost always means data tracking and a relentless stream of adverts no parent would knowingly sign up for.

The real breaking point came before a family holiday. My wife and I sat down with the kids to find a couple of simple travel games — expecting, at the very least, something honest and clean. Instead we found the exact patterns covered in this guide: video adverts and constant interruptions, forced account sign-ups, sneaky paywalls and accidental taps, and manipulative loops clearly built to keep kids hooked rather than entertained.

so I built an alternative.



14 · A NOTE FROM THE AUTHOR

From our kitchen table in Surrey, I started coding a small collection of simple, wholesome games — the kind we could play together, or the kids could enjoy solo. My own children became the chief testers and harshest critics. When other parents saw it and asked for a copy, that was the push to release it properly, as **Pumpkin Cat Games** (pumpkincatgames.com).

Pumpkin Cat Games is built on four non-negotiable standards:

Zero adverts

No banners, pop-ups, or video interruptions

Zero tracking

No behavioural monitoring, analytics, or data harvesting

Zero sign-ups

No accounts, emails, or logins required

Zero paywalls

Completely free to play, with nothing to buy, ever

It includes a PIN-protected parent gate, per-game access controls, and daily time limits — so the boundaries in this guide are already built in, not something you have to fight the app to get. It's designed in line with COPPA, UK & EU GDPR, and the ICO Children's Code⁵⁴, and it's free on Android now.

It won't solve every risk in this guide — other games' chat features and app stores in general still need the vigilance covered in Chapters 2–11. But it's one honest answer to the question this whole guide keeps circling back to: what would a game built for children, rather than built to monetise them, actually look like?

tap or scan to download

Download free on Google Play

play.google.com/store/apps/details?id=com.drew.games

More at pumpkincatgames.com



Before you tap “Install” – the two-minute check



PEGI or ESRB rating

Does it match your child’s age, not just their reading level?



Content descriptors

Tap through to see why it got that rating.



Search the game name plus “chat” or “scam”

A 30-second search surfaces known issues fast.



Permissions and Data safety on the listing

Do camera, microphone, location and contacts match what the game does?



Chat, voice or open multiplayer?

If yes, plan to disable or restrict it before your child plays.



Is it free?

If yes, assume it is ad- or purchase-funded and plan accordingly.

If any of these raise a concern, don’t install yet — dig further or look for an alternative.

Once it's installed — set this up before handing over the device

Set-up

- ✓ **Install or approve via Google Family Link**
not your own account
- ✓ **Require approval for downloads and purchases**
Family Link → Controls → Google Play
- ✓ **Remove saved card details**
from the device where possible
- ✓ **In the game itself: disable chat**
or restrict it to “friends only”
- ✓ **Set the profile to private**
turn off personalised ads and location sharing
- ✓ **Set a daily time limit**
in Family Link

Keep an eye on this — monthly is a good habit

-  **Play Store → Payments and subscriptions**
Budget and history — scan for small, repeated charges
-  **Family Link → Screen time**
Check play time and recently installed apps
-  **Ask what they're playing and who with**
A real conversation, not an inspection

Red flags, and who to call

Red flags (full detail in Chapter 10)

A single sign is rarely a crisis. A **cluster** of these, especially around a new online contact, is worth a calm conversation:

Secretive chatting



Mood swings tied to messages



Unexplained in-game currency or gifts



Withdrawal from things they used to enjoy

If something's gone wrong — keep this handy

Immediate danger

999

Suspected grooming or predatory contact

CEOP — ceop.police.uk/safety-centre

Bullying or general worry

NSPCC Helpline (adults) —
0808 800 5000
Childline (children) — 0800 1111

Unexpected purchase

Google Play order history → Report a problem (act quickly)

Sources.

Numbers in the text, like ¹, match the entries below, listed chapter by chapter. Links are clickable in the PDF.

01 Introduction

- 1 Ofcom**, “Top trends from our latest look at UK children’s online lives” (June 2025)
ofcom.org.uk/media-use-and-attitudes/media-habits-children/top-trends-from-our-latest-look-at-uk-childrens-online-lives
- 2 5Rights Foundation**, “New research reveals how children face financial harm online” (July 2025)
5rightsfoundation.com/new-research-reveals-how-children-face-financial-harm-online/
- 3 Ofcom**, “Children and Parents: Media Use and Attitudes Report” (March 2023)
ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/childrens-media-use-and-attitudes-2023/childrens-media-use-and-attitudes-report-2023.pdf
- 4 Ofcom**, “Children and Parents: Media Use and Attitudes Report” (April 2024) · also Ch 5
ofcom.org.uk/_data/assets/pdf_file/0025/283048/Childrens-Media-Literacy-Report-2024.pdf

02 Android’s built-in controls

- 5 Google For Families Help**, “Manage your child’s Google Play apps” · also Ch 5, 9
support.google.com/families/answer/7103028
- 6 Google Play Help**, “How to set up content restrictions on Google Play” · also Ch 7
support.google.com/googleplay/answer/1075738?hl=en
- 7 Google For Families Help**, “Set app time limits on your child’s device”
support.google.com/families/answer/15957417
- 8 Google Families**, “Family Link FAQ”
families.google/familylink/faq/
- 9 Google For Families Help**, “Purchase approvals on Google Play”
support.google.com/families/answer/7039872

03 Permissions and data

- 10 Android Help**, “Change app permissions on your Android phone”
support.google.com/android/answer/9431959
- 11 Android Help**, “Manage permissions from the privacy dashboard”
support.google.com/android/answer/13530434
- 12 Michigan Medicine**, “Advertising in kids’ apps more prevalent than parents may realize” (October 2018)
michiganmedicine.org/health-lab/advertising-kids-apps-more-prevalent-parents-may-realize

04 In-app purchases

- 13 Federal Trade Commission**, “FTC Sends Refund Payments to Consumers Impacted by Epic Games’ Unlawful Billing Practices”
ftc.gov/news-events/news/press-releases/2024/12/ftc-sends-refund-payments-consumers-impacted-epic-games-unlawful-billing-practices

SOURCES · CONTINUED

04 In-app purchases (continued)

- 14 **Epic Games**, “Epic FTC Settlement and moving beyond long-standing industry practices”
epicgames.com/site/news/epic-ftc-settlement-and-moving-beyond-long-standing-industry-practices
- 15 **Federal Trade Commission**, “Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges” (December 2022) · also Ch 5, 6, 9
ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations
- 16 **Google Play Help**, “Purchase verification for Google Play”
support.google.com/googleplay/answer/1626831?hl=en-GB

05 Chat and strangers

- 17 **ITV News**, “Mosque shootings and far-right skins: Teens playing Roblox exposed to extremist content” (November 2025)
[itv.com/news/2025-11-14/mosque-attacks-and-far-right-skins-roblox-teens-exposed-to-extremist-cont](https://itv.com/news/2025-11-14/mosque-attacks-and-far-right-skins-roblox-teens-exposed-to-extremist-content)
ent

06 Ads and dark patterns

- 18 **Dentons Commercial Litigation Blog**, “Dark times for ‘Dark Patterns’? Epic Games settles over unauthorized micro-transactions”
commerciallitigationblog.com/dark-times-for-dark-patterns-epic-games-settles-over-unauthorized-micro-transactions-and-user-interface-trickery-sort-of/
- 19 **Federal Trade Commission**, “\$245 million FTC settlement alleges Fortnite owner Epic Games used digital dark patterns”
ftc.gov/business-guidance/blog/2022/12/245-million-ftc-settlement-alleges-fortnite-owner-epic-games-used-digital-dark-patterns-charge
- 20 **Loeb & Loeb LLP**, “Fortnite Video Game Maker Settles FTC Privacy, Deception Claims for Record \$520 Million”
[loeb.com/en/insights/publications/2023/01/fortnite-video-game-maker-settles-ftc-privacy-deception-cl](https://loeb.com/en/insights/publications/2023/01/fortnite-video-game-maker-settles-ftc-privacy-deception-claims-for-record-$520-million)
aims-for-record-\$520-million
- 21 **Parent Coalition for Student Privacy**, “Google Lawsuit, COPPA, Investigating and Blocking Ad Trackers in Children’s Apps”
[studentprivacymatters.org/google-lawsuit-coppa-and-investigating-and-blocking-ad-trackers-in-childre](https://studentprivacymatters.org/google-lawsuit-coppa-and-investigating-and-blocking-ad-trackers-in-childrens-apps/)
ns-apps/
- 22 **Secure Privacy**, “Cookie Banner Dark Patterns: The New Manipulation Tactics Regulators Are Targeting”
secureprivacy.ai/blog/cookie-banner-dark-patterns-gdpr
- 23 **IAB Europe**, “TCF Vendor List”
iabeurope.eu/vendor-list-tcf/
- 24 **Springer Nature**, “‘Stay Out of My Way!': The Impact of Cookie Consent Notice Design on Young Users’ Decision”
link.springer.com/chapter/10.1007/978-3-031-35822-7_34
- 25 **EMARKETER**, “Over half of Gen Z and millennials often or always accept cookies”
emarketer.com/content/over-half-of-gen-z-millennials-often-always-accept-cookies
- 26 **PRIVO**, “Cookies, Consent & Children Prove a Challenge”
privo.com/blog/cookies-consent-children-prove-a-challenge

SOURCES · CONTINUED

07 Age-appropriate games

- 27 Google Play Help**, “Apps & Games content ratings on Google Play”
support.google.com/googleplay/answer/6209544
- 28 Nintendo UK**, “PEGI age ratings inform you at a glance”
nintendo.com/en-gb/Support/Parents/Age-Rating/The-PEGI-age-rating-system/PEGI-age-ratings-inform-you-at-a-glance/PEGI-age-ratings-inform-you-at-a-glance-854941.html
- 29 PEGI**, “Statistics about PEGI” (Ipsos/GameTrack study for Video Games Europe)
pegi.info/page/statistics-about-pegi
- 30 Play Console Help**, “Content rating requirements for apps, games, and the ads served on both”
support.google.com/googleplay/android-developer/answer/9859655

08 Screen time

- 31 SSS Learning**, “Gaming Addiction: Supporting Children at Risk” (citing Children’s Commissioner and Gambling Commission data)
sslearning.co.uk/safeguarding-articles/child-gaming-addiction
- 32 UK Parliament Education Committee**, “Screen time: impacts on education and wellbeing”
publications.parliament.uk/pa/cm5804/cmselect/cmeduc/118/summary.html

09 Privacy and accounts

- 33 Hudson Cook LLP**, “Mo Data, Mo Problems: Data Protection and Privacy Concerns for the Gaming Industry”
hudsoncook.com/article/mo-data-mo-problems-data-protection-and-privacy-concerns-for-the-gaming-industry/
- 34 National Cyber Security Centre**, “Online gaming for families and individuals”
ncsc.gov.uk/guidance/online-gaming-for-families-and-individuals
- 35 Roblox Support**, “Parental Controls Overview”
en.help.roblox.com/hc/articles/30428310121620
- 36 PlayStation Support**, “How to set parental controls on PlayStation consoles”
playstation.com/en-gb/support/account/ps5-parental-controls-spending-limits/
- 37 Xbox**, “Xbox family settings: peace of mind for parents”
xbox.com/en-GB/family-hub

10 Red flags

- 38 CPD Online College**, “Signs of Online Grooming to Watch For”
cpdonline.co.uk/knowledge-base/safeguarding/online-grooming-warning-signs/
- 39 BroadbandSwitch.uk**, “Warning Signs of Online Harm UK Parents 2026: How to Spot Trouble Early”
broadbandswitch.uk/online-safety/warning-signs/
- 40 NSPCC**, “Data shows how criminals are using private messaging platforms to manipulate and groom children” (November 2025)
nspcc.org.uk/about-us/news-opinion/2025/data-shows-how-criminals-are-using-private-messaging-platforms-to-manipulate-and-groom-children/

SOURCES · CONTINUED

11 If something goes wrong

- 41** CEOP (National Crime Agency), “Child Exploitation and Online Protection Command: make a report”
ceop.police.uk/ceop-reporting/
- 42** NSPCC, “NSPCC Helpline”
nspcc.org.uk/keeping-children-safe/our-services/nspcc-helpline/
- 43** Google Play Help, “Request a refund on Google Play”
support.google.com/googleplay/answer/15574897?hl=en
- 44** CBC News, “Google to refund \$19M US for kids’ mobile spending sprees”
amp.cbc.ca/news/business/google-to-refund-19m-us-for-kids-mobile-spending-sprees-1.2755769
- 45** Net Psychology, “Online Grooming: How Predators Manipulate Children (2026)”
netpsychology.org/online-grooming-how-predators-manipulate-their-victims/

12 Ongoing conversations

- 46** Stoilova, M., Bulger, M. & Livingstone, S., “Do parental control tools fulfil family expectations for child protection? A rapid evidence review of the contexts and outcomes of use” (Journal of Children and Media, 2023)
tandfonline.com/doi/full/10.1080/17482798.2023.2265512
- 47** Department for Science, Innovation and Technology, “Children’s circumvention behaviours online” (July 2026)
gov.uk/government/publications/childrens-circumvention-behaviours-online
- 48** Ghosh, A.K. et al., “Safety vs. Surveillance: What Children Have to Say about Mobile Apps for Parental Control” (CHI 2018)
doi.org/10.1145/3173574.3173698
- 49** Livingstone, S. et al., “Maximizing opportunities and minimizing risks for children online: the role of digital skills in emerging strategies of parental mediation” (Journal of Communication, 2017)
eprints.lse.ac.uk/68612/

13 Why safe gaming needs better games

- 50** 42matters, “Google Play Statistics and Trends 2026” (October 2026)
data.42matters.com/google-play-statistics-and-trends
- 51** Sensor Tower, “State of Mobile 2026” (January 2026)
sensortower.com/blog/state-of-mobile-2026
- 52** Plarium, “50 Revealing Mobile Game Monetization Statistics and Facts”
plarium.com/en/blog/mobile-game-monetization-statistics/
- 53** Game World Observer, “In 2025, the revenue of the mobile gaming market grew, but only slightly — analysis” (January 2026, citing Sensor Tower)
gameworldobserver.com/2026/01/21/in-2025-the-revenue-of-the-mobile-gaming-market-grew-but-only-slightly-analysis

14 A note from the author

- 54** Pumpkin Cat Games, “Child Safety Statement”
pumpkincatgames.com/child-safety-statement



Games built for children, rather than built to monetise them.

Built by a parent, for families

Zero adverts

Zero tracking

Zero sign-ups

Zero paywalls



tap or scan to download

Download free on Google Play

play.google.com/store/apps/details?id=com.drew.games

pumpkincatgames.com · Free on Android now

What about iPhone and iPad? Unlike Android, Apple requires an ongoing \$99/year developer fee, even for completely free apps that have zero adverts. As Pumpkin Cat Games is an independent passion project funded out of pocket, that recurring cost isn't viable right now. If circumstances change, or community support grows in the future, we would love to bring it to iOS!

Designed in line with COPPA, UK & EU GDPR, and the ICO Children's Code