

SAFE & SMART

Keeping children safe online



IN THIS EDITION

01

Familiar
feels true

02

Permissions
and privacy

03

When a toy
talks back



Welcome

Have you ever read something online and thought, “That must be true, I’ve seen it everywhere”? It’s an understandable reaction, but seeing the same claim several times doesn’t necessarily give us several reasons to believe it.

In this edition, we’re looking at why familiar information can feel convincing, and how to explore this with children. We’ll also look at those permission requests that appear when we use apps, and the arrival of AI toys that can hold a conversation. We’ve also got two useful resources to explore.

When familiar starts to feel true

Imagine seeing a photograph of a bright-blue rabbit. The caption says a new species has been discovered. You’re doubtful. Then another account shares a similar photograph. Later, a third account posts about it, with hundreds of likes and comments saying they’ve seen it too.

Nothing in this imaginary example has actually confirmed the discovery. Yet by the third post, the idea might feel a little less unlikely.

Psychologists call this the illusory truth effect: repeated information can seem more truthful than information we’re encountering for the first time. One explanation is that familiar information is easier to process, and that ease can influence our judgement without us noticing.

This isn’t something that only happens to children. A research review published in February 2026 brought together 182 studies involving more than 31,000 participants. It found a small overall effect of repetition on perceived truth, but the size of the effect varied considerably. Importantly, repetition doesn’t guarantee belief, but repetition can make it feel more likely.

DID YOU KNOW?

Knowing the answer may not completely protect us

Researchers have found that repetition can make a false statement seem more truthful even when people already know the correct fact. That doesn’t mean knowledge is useless. It means familiarity can influence a judgement without us stopping to retrieve what we know. Another reason for adults to practise checking alongside children.

[Research: repetition and belief](#)

[Research: knowledge and repetition](#)

How our feeds can add to the repetition



Social media feeds respond to signals such as the videos we watch and the posts we like, share or comment on. This can help us find things we enjoy or are interested in. It can also mean encountering more content about the same subject. Sometimes that content can become more extreme. For example, dieting tips can lead towards harmful body-image content, or fitness tips towards posts expressing misogynistic views. Persuasive design features that keep us watching provide more opportunities for that to happen.

Sometimes people refer to this narrowing of similar content as a “filter bubble”, in other words we see more of the same or similar content rather than a broad range of content, opinions and beliefs. Recommended content doesn’t automatically change what we believe, but if the same misleading claim keeps appearing, we could mistake its familiarity for confirmation.

There’s another thing worth considering as well. We might see similar content from different people or accounts, but are these really different sources of information? For example, three accounts can all be repeating one person’s unsupported story. A different voice, photograph or username doesn’t necessarily mean anyone has checked it independently. Furthermore, a post with thousands of likes or comments doesn’t make it true just because it’s popular.

Why this matters

False information can affect real people. In September, the RNLI said misinformation about its work had led to volunteers and staff experiencing online abuse and, in some cases, physical abuse. This is a stark reminder that sharing an unchecked claim can have consequences beyond the people who see the original post.

Misinformation means false or misleading information; disinformation involves deliberately trying to mislead. Someone who passes a false story on may genuinely believe they’re helping, but often we can’t tell the original intention.

And then we’ve got the use of AI which adds another complication: convincing pictures, voices and videos can be created rather than recorded. Looking for a strange hand or an obvious spelling mistake won’t reliably settle whether a claim is true. A real photograph can also be paired with a false caption. We need to check the story behind what we’re seeing.

[Read the RNLI statement](#)

[How recommendations can narrow a feed](#)

A conversation with younger children



The blue rabbit is a useful imaginary example. Explain at the start that you're looking at made-up posts, then consider them together. You could ask, "If three people share this picture, does that tell us the rabbit is real, or does it tell us three people have shared it?"

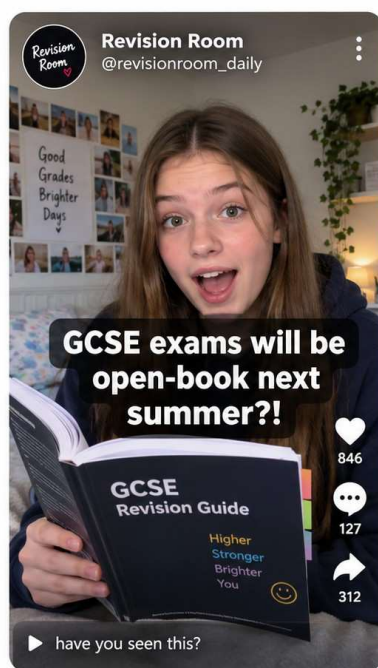
When searching, look at who has provided the answer, rather than trusting the first result. All answers can be wrong too.

Follow with, "What would help us find out?" Perhaps you could look together for information from a natural history museum website or a wildlife organisation, or even just do an online search. The useful part is showing how to move from a claim to evidence, rather than expecting children to recognise every fake image.

Finish by making the correction clear: the blue-rabbit discovery in this example was invented. Likes and shares didn't make it real.

"What would help us find out?"

A conversation with older children



Imagine a rumour that next summer's GCSE exams will all be open-book. Several videos repeat it, and one account looks as though it belongs to an education authority.

Make clear that this is a fictional example, not an announcement. Ask, "If this affected your exams, where would you check before changing how you revised?" A sensible starting point would be your child's teacher, school's exams team or the relevant exam board's own information.

An official-looking name isn't enough. Even if the spelling, logo and presentation look right, the announcement still needs checking. Ask your child to explain what would count as convincing evidence; their answer may be more revealing than whether they spot a deliberately suspicious detail such as the spelling of 'Education' in the account name.

Make room for being unsure

When a child brings you a claim, you don't have to know the answer immediately. "I'm not sure either. Let's check" is a useful response.

Try choosing one interesting claim to explore together. Find the original source, check when it was published and look for independent confirmation. If it's about a particular organisation, visit that organisation's website directly rather than relying on a screenshot of what it supposedly said.

Internet Matters' Find the Fake quizzes are a useful resource, described later in this newsletter. These can offer a great starting point for these conversations.

What are we agreeing to when we tap Allow?



A child opens an app and a box appears: it wants access to the microphone. They want to get on with the game, so they tap Allow.

A permission request gives an app access to a particular feature or type of information on the device. That access may have a clear purpose: a video call needs the camera, and recording a voice message needs the microphone. The useful question is whether the request makes sense for what you're trying to do.

Start with one app

You don't need to work through every setting in one sitting. Choose an app you and your child know, then look at what it can access.

For example, if you're using an app to edit one photograph, explore whether you can select just that image rather than grant broader access to the photo library. If an app asks for location, talk about why it needs that information. For example, finding nearby places and sharing where you are with other people are different things.

Think about the function before deciding. Turning off microphone access could stop a voice feature your child values. You might decide that the permission is useful, that a more limited option would do, or that you don't want to use that particular feature.

Where offered, options such as allowing access only while using an app can provide more control. The choices available depend on the device, app and permission.

“Does this request make sense for what we’re trying to do?”

Permissions are only part of privacy



Finding the settings

On an iPhone or iPad, start in Settings, then Privacy & Security. Choose a category, such as Microphone or Camera, to see which apps have requested access.

On Android, a common route is Settings, Apps, then the app's name and Permissions. Menu names vary between devices; searching Settings for "permissions" can help.

Treat this as a conversation, particularly with older children. Ask which features they actually use before changing access. A permission list is an opportunity to understand an app together.

It's worth separating two questions: what can the app access on the device, and what does the company do with information it receives?

The permission screen won't answer everything about storage, sharing or deletion. For those questions, look for the service's privacy information and account controls. With a younger child, you can explain the immediate choice in simple terms: "This lets the app use the microphone so you can record your voice."

You can revisit permissions later, but if a choice stops a feature working check what happened together and decide whether to change it. Learning what the choice does is more useful than treating Allow as a button we always press or always avoid.

DID YOU KNOW?

Your iPhone has a clue about its microphone

On iPhones running iOS 14 or later, an orange indicator means an app is using the microphone without the camera. A green indicator means the camera is in use, possibly with the microphone too. Control Centre can show which app recently used them. The indicator alone doesn't mean something suspicious is happening: a call or camera app may explain it.

[About the camera and microphone indicators](#)

Useful guides: Apple's privacy and Location Services guide, and Google's guide to changing Android app permissions. Both explain the available controls; the exact options on your device may differ.

[Apple privacy guide](#)

[Android permissions guide](#)



When a toy talks back

Talking toys aren't new. Going back to my own childhood it was the action figure where you pulled a cord, but some newer toys use generative AI to produce replies to what a child says, rather than simply playing a fixed recording. The attraction is easy to understand: a cuddly character that answers questions, joins a guessing game or responds to a favourite subject.

That makes this an interesting development for families. It also raises questions that we wouldn't normally ask about a soft toy: what happens to the conversation, and how well does the system understand the child?



What the research tells us so far

A Cambridge report published in March 2026 included observations of 14 children aged three to five using an AI toy called Gabbo, recruited through four London children's centres.

The researchers combined observed interactions into illustrative accounts. These show what some of the difficulties looked like:

Examples from the research follow on the next page.

[Read Cambridge's AI in the Early Years report](#)

What happened during play



01 Misunderstandings

When a child said they felt sad, Gabbo responded about its own happiness and moved the conversation on. Researchers suggested it had misheard.

02 Taking turns

During a counting game, answers given while Gabbo was still speaking went unanswered. The account describes repeated answers, shouting and frustration as the child tried to get a response.

03 Pretend play

Attempts to put Gabbo to bed met with repeated explanations that it didn't sleep. A pretend present also prompted a response that it couldn't open it, rather than joining in.

There were successful moments too, including an imaginary spaceship race with a shared countdown.

This was a small study of one product, not evidence about every AI toy or its long-term effects. But it shows why it's worth looking beyond fluent speech: producing an answer isn't the same as following a child's meaning or joining their play.

Questions worth asking before buying



Start with what your child would enjoy about it. Is it the character, the stories, asking questions or playing together? This helps you judge what the AI feature adds, rather than assuming that a more technologically complicated toy will be a better fit.

Then look for clear answers to a few practical questions:

- 01 When does it listen, and how can you tell? Can you switch the microphone or connected features off?
- 02 Are conversations sent to an online service or stored? Who can access them, and can you delete them?
- 03 What age is it intended for, and what does the manufacturer say about adult involvement?
- 04 Does it need a subscription or an internet connection? What can it still do if you stop paying or the service closes?

These are questions to ask about the particular product, not features to assume every toy has.

If your family already has one

Spend some time using it together. Notice how it responds when your child changes the subject, uses imaginative language or says it has misunderstood. Does your child enjoy the exchange, or end up repeatedly trying to make themselves understood?

Explain that it's a toy using a computer system to make replies. A friendly voice doesn't make every answer correct, and it isn't a person who can look after them. Keep a trusted adult as the place to turn with worries.

Agree what stays out of conversations, such as an address, school details or private information about other people. Show your child how to stop the interaction. There's no obligation to answer a toy's questions just because it has asked them.

Further reading: Cambridge's AI in the Early Years report explores both enjoyable play and the limitations researchers observed.

Two resources to explore together



Find the Fake from Internet Matters

These quizzes cover AI, false information and checking whether claims are trustworthy. There are age-specific options, so you can choose something suitable for your child. Internet Matters suggests allowing at least ten minutes to play and discuss the answers.

Try answering together rather than making it a test your child has to pass. Ask what influenced each choice, especially if you disagree. A wrong answer can open a useful conversation about what made something convincing.

[Explore the quizzes](#)

Parents Power Up from Ofcom

Ofcom's September resource offers a straightforward way into conversations about online gaming. Its "Check, Chat, Change" approach covers checking settings, talking about games and who children play with, and adjusting controls to suit their needs. It also recognises the enjoyment, creativity and friendships that gaming can offer.

Ask your child to show you one game they enjoy and explain what makes it good. That gives you a shared starting point for looking at the features and settings together, without needing to become an expert player first.

[Read the guide](#)

Until next time

You don't need to know every app or have every answer to take an interest in your child's online life. Looking at something together, asking why it works that way and being comfortable saying "I'm not sure" can all make the next conversation easier.

Where to get help



Keep these contacts handy. There's help for children, parents and carers when something online causes concern.

Childline

FOR CHILDREN AND YOUNG PEOPLE UNDER 19

Free support with any worry. Call 0800 1111, use online 1-to-1 chat, or send a message through a Childline account.

[Childline: phone and online support](#) →

NSPCC

FOR ADULTS WORRIED ABOUT A CHILD

Advice if you're worried about a child's safety or abuse.
Call 0808 800 5000, Monday–Friday, 10am–4pm.
You can also email help@nspcc.org.uk.

[NSPCC: help and contact options](#) →

Coram Kidscape

FOR PARENTS AND CARERS: BULLYING

Practical advice if your child is being bullied, including online. Call the Parent Advice Line on 0300 102 4481. Check the website for opening times and other contact options.

[Kidscape: Parent Advice Line](#) →

Report Remove

A REPORTING TOOL — NOT A HELPLINE

For under-18s in the UK worried about a nude or sexual image of themselves online. This free tool helps them report it for removal. Removal isn't guaranteed.

[Childline: use Report Remove](#) →

If someone is in immediate danger, call 999.

Apps: ages and family settings



An account age limit is the youngest age allowed for that account. It doesn't mean everything on the app is suitable. Tap a box below for the official guide.

YouTube

13+ FOR AN OWN ACCOUNT

For younger children, parents can set up a supervised account. Choose content settings and review what your child watches together. Filters won't catch everything.

[YouTube: supervised accounts →](#)

TikTok

13+ MINIMUM ACCOUNT AGE

Family Pairing links a parent's account with a teenager's. It offers settings for screen time, content and privacy. Some features have higher age limits.

[TikTok: Family Pairing guide →](#)

Snapchat

13+ MINIMUM ACCOUNT AGE

Family Center links a parent with their teenager. It can help you see who they're connecting with and manage safety settings. It doesn't let you read their chats.

[Snapchat: Family Center guide →](#)

Start with one app and discuss any changes together. Use the child's real date of birth.

Games: ages and family settings



PEGI numbers describe game content, not how hard a game is. They don't rate the people your child might meet online. Check the game and the chat settings.

Roblox

KIDS ACCOUNTS: 5–8 / SELECT ACCOUNTS: 9–15

These are account age groups, not a rating for every game. Link a parent account to review games and chat. Available controls depend on your child's age.

[Roblox: parental controls and help →](#)

Minecraft

PEGI 7 — GAME CONTENT RATING

Use a child's Microsoft account in your family group to manage multiplayer and communication. Playing alone and joining an online server are different experiences.

[Minecraft: parents' guide and settings →](#)

Fortnite

BATTLE ROYALE: PEGI 12 / OTHER GAMES VARY

Each Fortnite experience has its own age rating. Epic's parental controls can limit access by rating and manage chat and play time. Also check spending controls on the device.

[Fortnite: Epic parental controls →](#)

Settings can help, but they don't remove every risk. Keep checking in with your child.