digitalsafety
DIGITAL SAFETY FOR ALL

October 2026!



ONLINE SAFETY NEWSLETTER

October 2026

WELCOME TO EDITION THREE!

Welcome to the third edition of the Digital Safety Online Safety Newsletter.

As we move further into the autumn term, online safety continues to be an important part of school life. The digital world children and young people are navigating is changing quickly, and schools are increasingly being asked to consider not only what pupils are accessing online, but how technology, algorithms and emerging online behaviours can affect their safety and wellbeing.

In this edition, we're looking at some of the issues we think schools, parents and carers should have on their radar right now.

We explore how filter bubbles can shape the information children see online and why encouraging critical thinking and a wider range of perspectives is important.

We also look at fake livestream giveaways and online scams targeting children, including the risks around in-game currencies, payments and sharing personal information.

Alongside this, we'll be sharing details of our upcoming School Cyber Safety & Standards Conference 2026, as well as an update on LOOP, our National Lottery-funded community project.



Stuart Younger Cooper, Digital Safety CIC

This month:

- **Understanding filter bubbles and how they affect children**
- **Online giveaway scams and in-game currencies**
- **School Cyber Safety & Standards Conference 2026**
- **An update on the LOOP community project**

Our aim remains the same: to cut through the noise and turn current online-safety developments into clear, practical information that schools and families can actually use.

Digital safeguarding isn't something that sits with one person or one department. It requires ongoing conversations between leadership teams, safeguarding leads, IT staff, teachers, governors, parents and, importantly, young people themselves.

We hope this month's edition gives you useful information and practical prompts for those conversations.

digitalsafety
DIGITAL SAFETY FOR ALL

October 2026!

ONLINE SAFETY NEWSLETTER



October 2026

The four attack types AI is amplifying most

Phishing, ransomware, social engineering, and the new one most schools aren't ready for yet: vishing. We cover what each looks like in 2026, and the practical signals your staff should be trained to spot now.

How the same tools work for your defense

Adaptive phishing simulations, AI-assisted policy work, smarter awareness training, and benchmarking against the standards that matter for your territory. The same capabilities that make attackers faster are also making schools safer.

Practical steps to get started

A prioritised running order for the steps you can take, wherever you are in your cybersecurity journey. Start with the move that gives you the biggest risk reduction for the smallest spend, and build from there.

Need more help? Click the link below and let our team of experts at Digital Safety help keep you secure.

Click here to contact a cyber specialist

Or email us at info@ds-cic.com

Why Filter Bubbles Are Harmful to Children (*and How Parents Can Help*)



The internet is an amazing tool that connects us to endless information, cultures, and perspectives. But over the past decade, how that information flows to us has fundamentally changed. Behind the scenes, invisible algorithms shape the content we see every time we scroll, click, or search. While they make our online experience feel personal, they also trap us in what's known as a filter bubble.

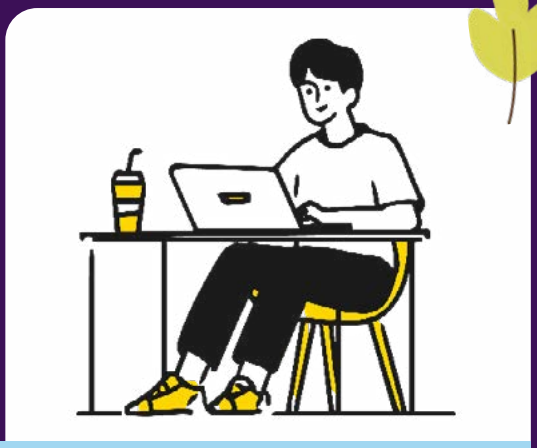
As parents and caregivers, understanding this phenomenon is vital; not only for our own awareness but for guiding young people navigating the digital world. Here's what you need to know and what you can do about it.

What Is a Filter Bubble?

The term "filter bubble," coined by internet activist Eli Pariser, refers to the personalised

digitalsafety
DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



October Edition

WHAT ARE FILTER BUBBLES?

online universe created by algorithms that decide what you see, and what you don't. Here's how it works:

- Algorithms analyse your behaviour: Platforms like Google, Facebook, and YouTube monitor what you click, watch, or like.

- They prioritise content you'll engage with: The goal is to keep you scrolling longer so they can serve more ads and maximise profits.

- They filter out opposing views: By showing you what you already agree with or enjoy, algorithms avoid exposing you to challenging or conflicting information.

While it might feel convenient to see content tailored to your tastes, it can lead to unintended consequences, like reinforcing biases, narrowing worldviews, and even fostering divisions.

Why Should Parents Care?

For children and teens, filter bubbles can significantly shape their understanding of the world. Here are some potential pitfalls:

1. Warped Reality: Being exposed only to like-minded ideas can make it harder for young people to empathise with others or consider opposing viewpoints.

2. Echo Chambers: Constant reinforcement of beliefs creates a skewed reality where differing perspectives are dismissed or vilified.

3. Manipulation Risks: Platforms use these algorithms to sell products, ideologies, or even misinformation, making children particularly vulnerable to exploitation.



How to Break Free from the Filter Bubble

1. Teach Critical Thinking: Help your child question the source of their information. Who created it? Why? Encourage them to research multiple perspectives on any topic.

2. Diversify Information Sources: Show your children how to explore content from various platforms, not just their favourite apps or websites. Subscribing to reputable news outlets or reading physical books are great starts.

digitalsafety
DIGITAL SAFETY FOR ALL

SETTING THE EXAMPLE



October Edition

3. Turn Off Personalisation: Many platforms allow you to adjust settings to limit algorithmic filtering. For example:

- Use "incognito mode" for Google searches.
- Turn off autoplay features on YouTube and other platforms.
- Avoid relying exclusively on curated news feeds from social media.

4. Follow Diverse Accounts: On platforms like Instagram or X, encourage your child to follow accounts that offer different perspectives. It's a simple way to expose them to broader views.

5. Have Open Discussions: Talk openly about the idea of filter bubbles. Sharing how algorithms work can demystify the process and empower kids to make smarter online choices.

Setting the Example

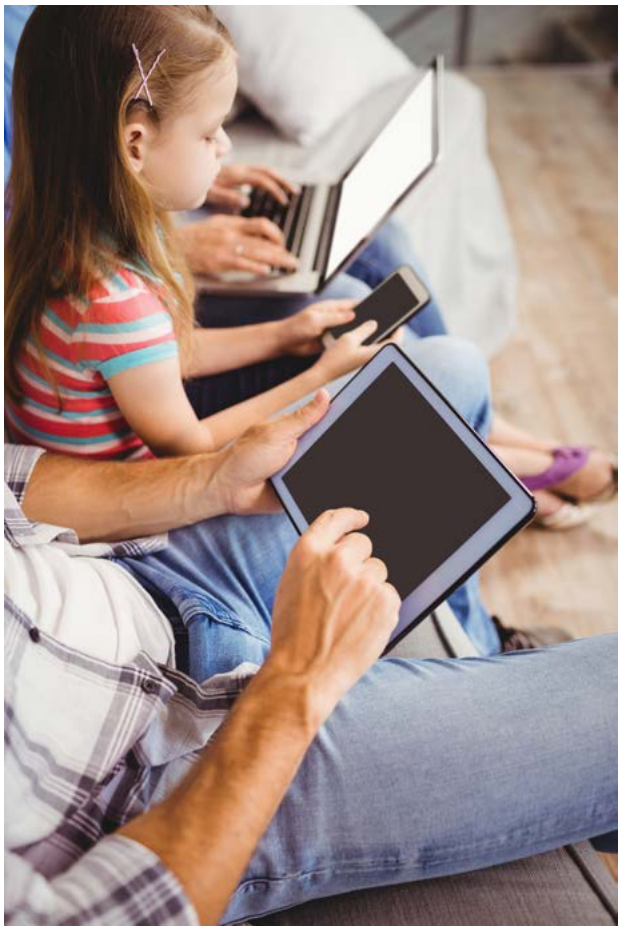
As parents and caregivers, we're also navigating filter bubbles in our own lives. Modelling behaviour, such as engaging with different perspectives respectfully or exploring diverse information sources, can profoundly influence young minds.

By actively stepping outside of our online comfort zones, we show children that learning, growth, and empathy come from challenging our own ideas and seeking to understand others.

Let's work together to raise a generation that uses technology not just for convenience but for building a more informed, compassionate, and connected world.

Stay curious, stay critical, and stay open!

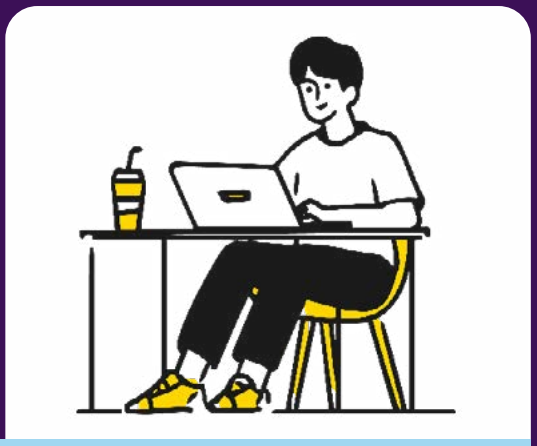
Learn about filter bubbles here



digitalsafety

DIGITAL SAFETY FOR ALL

WHERE DOES DATA GO?



October Edition

YouTube "Giveaway" Scams Targeting Children

A growing trend on platforms such as YouTube and TikTok is seeing children targeted through fake livestream giveaways, particularly those linked to in-game currencies such as Robux from Roblox. These streams are often designed to appear in short-form video feeds and use looping pre-recorded clips to hold attention. Common examples include fake countdowns, impossible "spot the difference" games, or staged moments designed to keep viewers watching.

Once enough viewers join, the livestream typically changes into a "giveaway". Children are encouraged to send paid stickers, gifts, or donations in exchange for promises of free Robux or other rewards. In many cases, the same usernames repeatedly "win" the giveaway, revealing that the stream is simply replaying the same video on a loop. Because payment methods are often already linked to devices, younger children may not fully understand that real money is being spent.

There are also wider safeguarding concerns. Some children may post their usernames publicly in livestream chats, creating opportunities for unwanted contact or further scams through gaming platforms.

For parents and schools, the key message is simple: if a creator is demanding money or promising rewards in exchange for donations, treat it with caution. Encourage children to check with a trusted adult before spending money online and remind them that legitimate creators do not usually pressure viewers into sending payments.

Children who encounter these streams should avoid engaging with the creator and instead report the content using YouTube's "Spam or misleading" reporting option.

Further reading and guidance:

- YouTube Guidance on Scams
- Reporting on YouTube
- Livestream Scams
- Example Video Livestream Scam

This type of scam is evolving quickly, but the core safeguarding message remains unchanged: if something online promises rewards for sending money, especially under pressure or urgency, it should be treated with suspicion.

digitalsafety
DIGITAL SAFETY FOR ALL

October 2026



SAFER GAMING

October 2026

SAFE ONLINE GAMING WITH OUR EXPERT GEORGE



George Spour, Digital Safety CIC

Body Cam; The hyper-realistic shooter going viral on TikTok, and why it's fuelling a new 'is this even real?' problem

What is it?

Body Cam is a multiplayer first-person shooter built in Unreal Engine 5 by Reissad Studio, a small French indie team. It launched into Steam Early Access on 7 June 2024 and reportedly sold around 800,000 copies within its first month. It's back in everyone's feed now because a major content update landed on 2 September 2026, adding new weapons, animations and a map.

Why it looks so real

The entire selling point is realism. The developers studied genuine police bodycam footage to copy its fisheye lens distortion, handheld camera shake, restricted field of view and even pixelated faces, the look of real footage that's been redacted before release.

That authenticity is the appeal for players, and exactly why short clips get mistaken for the real thing when they're shared without context.

Worth noting: this is a different incident to the well-known 2022 leak, where a British teenager was later convicted for his part in a hack carried out by the Lapsus$ group. That case is closed and this one is still unfolding.

The September 2026 update pushed that realism beyond visuals. Players now carry a Tactical Tablet in-game, a physical device rather than a pause menu, to manage loadouts and gadgets, including new FPV (first-person-view) reconnaissance drones and RC vehicles with a full manual 'Acro' flight mode that mirrors real drone flight physics closely enough that real-world FPV pilots report an advantage flying them. It's that mechanical, not just visual, attention to detail that's earning Body Cam a reputation as one of the more convincing tactical simulators on PC, on top of its looks.

The misinformation problem

This isn't the first 'bodycam-style' game to cause confusion. A similar (but separate and still unreleased) game, Unrecord, first went viral in October 2022 when an early clip racked up almost 10 million views; viewers, including well-known industry

digitalsafety
DIGITAL SAFETY FOR ALL

September 2026



SAFER GAMING

October 2026

figures, openly doubted it was gameplay at all. Now that Body Cam has actually shipped, its own clips circulate on TikTok and YouTube Shorts stripped of any game context, feeding a whole trend of 'is this real bodycam footage or a game?' videos, some deliberately left ambiguous for engagement.

What families and staff can do

No need for alarm, this is a media-literacy moment, not a crisis. 'Education without doom and gloom' means naming the risk plainly and pairing it with something practical:

- Ask how they'd check a clip, not just whether they saw it.
- Model checking the original account/ source before reacting or sharing.
- Treat 'it looks real' as a reason to check, not a reason to believe.
- Remember: the game itself isn't dangerous to know about. The skill that matters is verifying before believing.

Quick facts

- Developer: Reissad Studio, a small indie team in France
- Engine: Unreal Engine 5
- Platform: PC (Steam), Early Access only
- Launched: 7 June 2024
- Latest update: 2 September 2026 ("Locked & Loaded")
- Content: Steam's own listing flags "shooting and killing events"/gunfights
- Age guidance: no formal PEGI/ESRB rating yet (still Early Access): press consensus places it well above primary age
- Often confused with: Unrecord, a similar-looking but unrelated, still-unreleased game



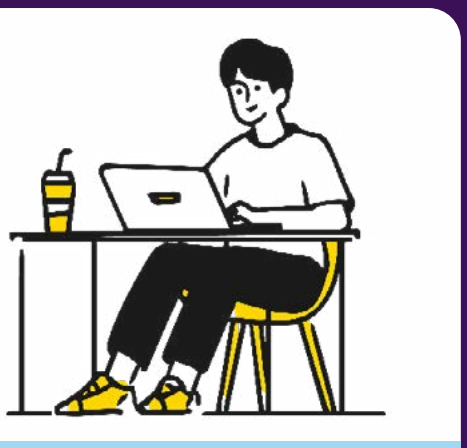


Want to understand Body Cam and the games your pupils are playing? George offers bespoke sessions for teachers and senior leaders on all things gaming! Get in touch to find out more.

digitalsafety
DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER

SAVE THE DATE!



October Edition

"*Preparing Schools for a Safer Digital Future*"

Barbara Spooner, MBE
CEO, Digital Safety CIC



School Cyber Safety & Standards Conference 2026

Helping Schools Prepare for the Future of Digital Safety

Thursday 15 October 2026
The Sjøvoll Centre, Durham

As schools continue to embrace technology in teaching, learning and administration, the demands around cyber security, online safety and digital governance have never been greater.

Join Digital Safety CIC and Framwellgate School Durham for a practical, informative conference designed specifically for education leaders. Bringing together experts from across the education and cyber security sectors, the event will explore the latest threats, share lessons learned from real incidents and provide practical guidance to help schools strengthen their digital resilience.

The conference will also look ahead to the Department for Education's Digital and Technology Standards, helping schools understand the steps they can take now to prepare for future requirements.

Who should attend?

- Headteachers and Senior Leadership Teams
- School Business and Operations Managers
- IT Managers and Network Leads
- Governors and Trustees
- Multi-Academy Trust Leaders
- Local Authority Education Teams

What you'll gain

- Practical cyber security guidance for schools
- Updates on emerging digital threats
- Advice on meeting DfE Digital and Technology Standards
- Best practice from experienced education and cyber professionals
- Networking opportunities with colleagues from across the sector

Date: Thursday 15 October 2026
Time: 10.00am – 3.00pm
Venue: The Sjøvoll Centre, Durham

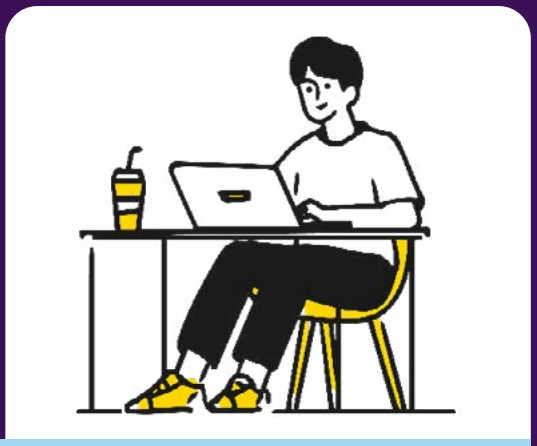
Attendance: £55 per person (includes lunch and refreshments)

To book your place, click the Eventbrite link below or email events@ds-cic.com, where a member of the team will be happy to assist with your booking.

Book your TICKETS here

digitalsafety
DIGITAL SAFETY FOR ALL

ONLINE SAFETY NEWSLETTER



September Edition

Help us shape a new way to share resources locally



Barbara Spooner, MBE
CEO, Digital Safety CIC

Digital Safety CIC is developing LOOP: Linking Opportunities, Organisations & People, a National Lottery funded project working with local organisations to help families share things like food, clothing (including school uniforms), household items and digital support more easily within the community.

To make sure LOOP actually works for local families, we'd love to hear from you. We've put together a short, completely anonymous questionnaire about how you currently find or share resources locally, and what would make this easier, whether that's something you sometimes need, something you're able to give, or both. It takes just a few minutes to complete, no personal details are collected, and your answers will directly shape the new platform we're building.

If you're able to spare a few minutes, you can complete the questionnaire here:

Help us here

Thank you for helping us build something that genuinely reflects what local families need.

Or scan the QR code below

LOOP Community Questionnaire

WISHING YOU ALL A HAPPY & HEALTHY AUTUMN!