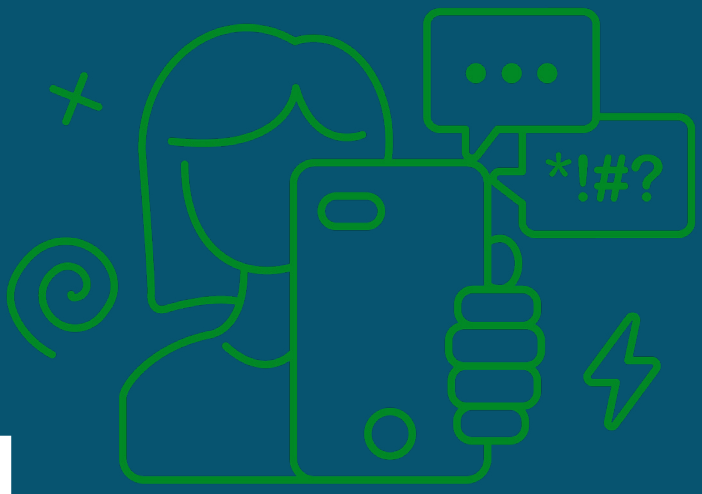
NSPCC




# Targeting Girls Online

## How online services enable the abuse and harassment of girls

By PA Consulting and NSPCC

# Contents





# Content advisory

This report explores sensitive issues and is designed to expose various harms that children may experience online. Readers are advised to read the content warning below and reflect on the likelihood that some of the topics, and the specific examples used to illustrate abusive communication, may cause them distress. Additional content warnings have been inserted before images that readers may find upsetting.

No children were involved in this study. Instead, girls' exposure to risk was explored by creating fake accounts for a fictitious 14-year-old character on 10 online services. The character is not based on any specific real person. The accounts were created and managed by adult researchers and were closed when the study came to an end.

The decision was taken not to disclose the names of the 10 online services investigated as part of the study. Images of screenshots have been substantially edited to prevent the identification of the services.

Content warning: This report contains references to child sexual abuse, intimate image abuse, online harassment, misogynistic comments, and a range of other types of abusive communication. Some images contain graphic language and fabricated scenarios that were designed to represent realistic examples of abusive communication that a girl may receive.

If you feel distress as a result of the issues raised in this report, you can contact the Samaritans for free at any time on 116 123 or jo@samaritans.org

If you believe that a child is being sexually abused or groomed online, you can contact CEOP to make a report: www.ceop.police.uk/ceop-reporting/

You can find out more information about technology-facilitated child sexual abuse by visiting The Marie Collins Foundation.

**If you are concerned about the safety or wellbeing of a child, please contact the NSPCC Helpline on 0808 800 5000 or help@NSPCC.org.uk.**

## About PA Consulting

PA has been working with UK and international governments, law enforcement agencies, regulators, and third sector partners since 2014 to understand how online harms are evolving globally (considering offender and victim behaviours, technology developments, and socio-economic factors).

In 2018, PA were the only professional services consultancy to respond to the UK Government's first consultation on online harms regulation. Since then, PA has continued to work with a range of UK public sector entities to prepare for online safety regulation, including with Ofcom on its 'A-SPARC' model of online platforms to inform the regulation of Video Sharing Platforms (VSPs), and the National Crime Agency.

PA has extensive expertise on the topic of children's safety online, which has developed and grown since facilitating the first series of multi-sector workshops convened by the UK Government in 2014 to come up with potential solutions to improve children's safety online. PA is also a founding industry partner of the WeProtect Global Alliance and has developed all four editions of the Global Threat Assessment of Child Sexual Exploitation and Abuse online (in 2018, 2019, 2021, and 2023).

Through work across the defence and security sectors, PA has a complementary, in-depth understanding of other high-threat harms, such as terrorism, violent extremism and hate speech, as well as of the methods, technologies, and tools used by the platforms who host user-generated content to detect, assess, block, and remove harmful material.

## Acknowledgements

Marcus Wright (PA Consulting) is the main author of this report, with contributions and editing by Eleni Romanou (NSPCC). The NSPCC would like to thank the team at PA Consulting for designing and carrying out the research, with special thanks to Marcus Wright, Yasmin de Silva, Patrick Cronin, Johnny Gilbert and Laura Suggitt. We are grateful to the subject-matter experts who contributed their time to interviews and to brainstorming and validating the proposed solutions. Our thanks also to internal NSPCC reviewers, and to the two external peer reviewers for their anonymous feedback on an earlier version of this report.

The NSPCC is an independent charity funded overwhelmingly by voluntary donations. The NSPCC is very grateful for the generous support from the Oak Foundation who made this research possible.



# Glossary

**Abusability testing:** A type of evaluation of technology products, which explores their vulnerability to abuse. It involves testing tools and features to discover whether and how they can be used to facilitate or enable harms to users.

**Avatar:** A character representing the user in an online space, that is often highly customisable.

**Bio:** A brief personal description or summary that users add to their profiles, often including details like interests, profession, or other identifiers, to introduce themselves to others.

**Contact risks or online abusive communication:** Online experiences of children involving the receipt of risky or harmful communication, such as sexual harassment, sexual solicitation, asking for sexual images, sending unsolicited sexual images, technology-assisted child sexual abuse, bullying, threats, extortion or hate speech.

**Dark patterns or dark design:** Design techniques that de-emphasise, obscure or make ambiguous more privacy-preserving options – for example, making opt-out buttons smaller and lower contrast.

**Generative AI:** A range of machine learning technologies that can generate new content (images, videos, text, and audio) in response to user prompts.

**Immersive technologies:** A range of technologies that blend the physical world with three-dimensional (3D) digital spaces, making users feel 'present' and immersed in the sights and sounds of digitally simulated scenarios.

**Platform:** A service that enables users to access user-generated content and facilitates user-to-user interaction (for example, social media or messaging apps). In this report, the terms 'platform' and 'online service' are used interchangeably.

**Perpetrator:** A user who carries out a harmful act.

**Safety-by-design:** A proactive and preventative approach to designing digital products that aims to ensure the burden of safety does not fall solely on the user, that products and services align with the best interests of users, and that services enhance user trust, awareness and understanding of the importance of user safety. According to safety-by-design principles, service providers need to anticipate, detect and eliminate online harms to users before they occur.

**User:** An account or profile belonging to an individual who is registered on a platform.

# Foreword from the CEO

**"We cannot wait any longer to take decisive action to better protect children online.**

**Technology companies must accept the scale of harm on their services and finally put children's safety first."**

The online world is a vital part of children and young people's lives. At the NSPCC, we regularly hear first-hand how these spaces are valued for creativity and play, community and learning, and much more. At the same time, we know that online services continue to put children at great risk. Young users on social media sites, gaming platforms, and messaging apps are regularly exposed to illegal behaviour, harmful content, and dangerous practices.

While all children can face harm, we know that many forms of online abuse and harassment disproportionately impact girls. Data we have collected at the NSPCC shows that four-in-five victims of online grooming cases are girls. Girls are more likely to receive unwanted sexual imagery online, and to have their images shared without consent. And over half of girls and young women report receiving sexist comments about themselves online.

The NSPCC commissioned PA Consulting to better understand how the design of online services shapes girls' experiences and, crucially, what needs to change to better protect them.

Using fake accounts for a fictious 14-year-old-girl, the research showed that the design choices built into the entire user journey of even the most popular platforms are putting girls at risk of abuse and harassment from malicious actors. Whether girls are creating new profiles, connecting with other users, or making use of functionalities like livestreaming, services have consistently failed to integrate appropriate safeguards.

Since I have joined the NSPCC, I have become all too familiar with the scale of harm children face online. So, while I found these findings deeply worrying, I was not shocked by them. It is clear to me that many tech companies have dragged their feet on making their sites safer, with devastating consequences for children and families.

Importantly, however, this report offers a way forward too. The report shares 27 solutions – positively, some of these are already included in Ofcom's Illegal Harms Codes. Implementing the rest in full would plug key gaps in existing protections and make a real impact on the experiences children have online. The technical solutions are there; now, we must see the will and ambition to take them forward.

This research has been done through the lens of a teenage girl, with a particular eye to the harms they are likely to experience online – but the solutions set out in this report would make a difference for all children. We need better safeguards for young users. We must also do a much better job of identifying children online, so they can benefit from protections and be supported to have age-appropriate experiences.

I thank PA Consulting for undertaking this research on the NSPCC's behalf. We are grateful for the expertise and care they brought to this work. As a result of their efforts, this report will be invaluable in helping to drive forward change for girls online.

We cannot wait any longer to take decisive action to better protect children online. Technology companies must accept the scale of harm on their services and finally put children's safety first. From Ofcom and the Government, we need ambitious and robust implementation of the Online Safety Act, holding services accountable for delivering transformational change. It is no less than families expect, and children deserve.

Chris Sherwood
Chief Executive Office
NSPCC

NSPCC



# Executive summary

This research focuses on girls' risk of being targeted by strangers with abusive online communication. It explores how malicious actors can exploit the design of online services that are popular with children to recognise which users are young and female, and to direct abuse at them. Abusive communication might take the form of sexual harassment, sexual solicitation, demanding sexual images, cyberflashing, technology-assisted child sexual abuse, bullying, threats, or hate speech.

The study takes as its starting point the fact that girls are disproportionately victimised online and that girls' user journeys on online services deserve to be studied in their own right. It proposed that specific design features of platforms can facilitate or promote abusive communication and set out to identify what these features were.

The design of 10 platforms was explored using fake accounts for a fictitious 14-year-old girl user. A combination of methods was used to understand the interplay between design, victimisation and perpetrator tactics: these included feature mapping and practical experimentation on the 10 platforms, desk research, and interviews with subject matter experts.

The research identified six areas of design that are vulnerable to exploitation by malicious actors. Within these areas, 19 features were pulled out as being particularly risky to girls, in that they enable service users to identify girls on the platform and make it possible – and sometimes easy – to approach girls and direct abuse at them. The report provides examples to illustrate how these design features can put girls at risk.

### Online profile

- The permanent visibility of basic identifiable information about the user
- The unrestricted ability to edit bios to include personal identifiable information
- The availability of highly gendered avatars
- The lack of settings to configure the presentation of curated content to other users

### Searching for other users

- The ability for adult users to see child users in their search results
- Children being recommended to adults as suggested contacts*
- The ability to view a child's list of connections*

### Connecting with others

- The ability of adults to send connection requests to child users
- Adults being recommended to children as potential connections during registration
- The display of mutual connections*
- The ability to be added or invited to group chats by others, without the user's permission and with little indication of the group's subject matter or membership
- The reduction in visible safeguards after a connection is made between users

### Direct messaging

- The ability to send or receive direct messages between adults and children*
- The ability to send abusive or inappropriate content without detection, prompts, blurring, or blocking
- The ability to send contact details through direct messages

### Livestream and in-game chat

- The ability for young children to have live video chats (and livestream) with other users
- Under-powered privacy and safety settings related to in-game chat features

### Gifting and rewards

- The ability to purchase and email electronic gift cards directly to children's personal email accounts
- The ability for adult users to purchase and gift paid memberships to children

The measures introduced in Ofcom's Illegal Content Codes of Practice partially address several of the risks listed above (where this is the case, a feature is marked with an asterisk). But Ofcom's measures are not sufficient on their own to protect girls from abusive communication from strangers. A further 27 design solutions were proposed to complement Ofcom's measures: these are practical changes that technology companies can make without undermining the basic functionality of their platforms, which will help protect girls from online contact risks.

The solutions include limiting the visibility of some types of information, restricting specific functionalities, introducing new protective features, revising the degree of customisation available, and removing dark patterns from design. A full list of solutions is presented in Chapter 9 of this report.

The risky design features identified here are part of a broader, systemic flaw in the design of online services, whereby children's safety, and the social and developmental factors that play a part in their online behaviour and interactions, are largely overlooked. This was clearly evidenced across the 10 platforms, in that none reliably distinguished child users from adult users, there was little attempt to offer age-appropriate experiences, and only some offered child users the highest safety settings by default. Overall, the platforms did not seem to be designed with child users in mind. On the contrary: the research showed examples of platforms that prompted the 14-year-old fictitious girl user to enter personal information that would be visible to strangers (see Chapter 2); where strangers were able to find her and identify her as a girl (see Chapter 3); where she was encouraged to connect with others and where others were able to connect with her (see Chapter 4); and where users who she may be connected to but barely know could communicate with her directly (see Chapters 5 and 6) or send her gifts (see Chapter 7). The responsibility to resist the platform's invitations to share her information and to reject approaches from strangers was placed almost entirely on the girl.

The most effective way to protect girls from abusive communication from strangers is the wholesale adoption of a safety-by-design ethos and the implementation of child-centred design principles. Technology companies must give due consideration to the rights and needs of child users, and design digital products accordingly. In the meantime, implementing the 27 solutions proposed in this report will go some way to protecting girls from malicious actors who may want to target them with abuse.



## Recommendations

### Ofcom

- Include all 27 solutions in the next iteration of the Illegal Harms Codes and, where appropriate, the Protection of Children Codes of Practice.
- Develop best practice guidance to services on how they should adapt protections to safeguard children of different ages and provide age-appropriate online experiences.

### UK Government

- Legally empower Ofcom to require services to use highly effective age assurance in order to uphold their minimum age limits and deliver age-appropriate experiences.
- Reaffirm the commitment to protect girls online in the upcoming Violence Against Women and Girls (VAWG) Strategy and strengthen protections in private messaging and real-time user-to-user interactions.

### Technology sector

- Commit to implementing all 27 solutions, operationalising them effectively for each platform.
- Conduct gendered risk analysis and abusability studies of digital products before rolling out any new features or functionalities.

### Researchers

- Conduct research on online harm that focuses specifically on girls, treating girls as a group in their own right.
- Investigate girls' user journeys through digital services to develop our understanding of online VAWG and intersectional experiences of abusive communication.
- Measure the scale of girls' victimisation and polyvictimisation through a large-scale prevalence study of child abuse in the UK.

# 1 Introduction

Gender-based violence affects at least one-in-12 women in the UK each year,[1] with abuse beginning early and perpetuated through harmful stereotypes. Relative to their male counterparts, girls face disproportionate risks of harassment, abuse, and exploitation, both offline and in the online world. Girls report feeling unsafe in public, at school, and online, with 93 per cent agreeing they do not feel completely safe in public spaces and only nine per cent feeling safe online.[2]

While online platforms offer girls opportunities for connection, they are also an arena for misogynistic, inappropriate and abusive communication from other users. The internet enables malicious actors to send abusive communication from a distance and engage in a range of abusive behaviours while maintaining their anonymity. Online abuse can also be automated, allowing perpetrators to significantly scale-up the number of their targets or volume of abuse against an individual. Abusive material is exceedingly difficult to eradicate once it has been shared online and this permanence can facilitate continued revictimisation.[3]

Girls bear the brunt of abusive online communication. Over half of girls aged 13–21 report receiving sexist comments about themselves online.[4] Online bullying is significantly higher among 10–15-year-old girls than among boys of the same age.[5] Similarly, online sexual risks are more common among girls than boys, including online sexual harassment, most types of intimate image abuse, and technology-assisted child sexual abuse by adults.[6] Research by Ofcom suggests that girls aged 16–18 are particularly likely to experience risky and abusive types of online communication.[7] These risks impact girls' psychological wellbeing, education, and future opportunities, while reinforcing societal inequality.

Despite this, most research (bar a few notable exceptions [8,9,10,11]) continues to conceptualise and measure online harm at the population level rather than trying to understand the specific experiences of girls. This research takes as its starting point the fact that girls face a unique configuration of risks in the online world, differing in scale and nature to the set of risks faced by boys. Girls' interactions with online spaces, therefore, deserve to be studied in their own right. Girls have a distinctive victimisation profile when it comes to abusive online communication, and the factors and conditions that lead to this should receive focused attention.

## Aims of the research

What girls do online, and what other users can do to girls, is shaped, enabled, and constrained by the ways in which online services are designed. This study hypothesised that specific design features can facilitate or promote behaviours in users that can adversely affect girls. It is these types of features that were of specific interest to the research.

The research aimed to explore the design of online services that are popular with children, and to pick out design features that malicious actors can exploit to identify and target young female users with harmful or abusive communication. Exploring design features in this way and testing if they can be abused to cause harm is sometimes known as 'abusability testing'.[12]

The research also aimed to generate recommendations for design changes that can mitigate risks to girl users, and which could be implemented by online service providers without unduly affecting the platforms' essential functionality. The proposed changes are intended to complement the measures proposed by Ofcom to protect users from illegal content and activity.[13]Ofcom's Illegal Content Codes of Practice were published while the research was taking place and came into effect in March 2025 through the Online Safety Act. The codes set out the measures that technology companies need to take to tackle online grooming, and many involve service providers making changes in the design of their services. The measures include the following:

- preventing child users' location, friends and connections being visible to other users
- preventing child users appearing in other users' network expansion prompts
- preventing child users from receiving direct messages from other users who they are not connected with
- giving child users the chance to actively confirm that they want to receive a message from someone they are not connected with when using services that do not have user connection functionality
- giving child users relevant supportive information at critical points in their user journey to allow them to make more informed choices.

Ofcom's measures will, in themselves, go some way to reducing girls' risk of receiving abuse from other users. The present research set out to discover what additional design changes are needed to further safeguard girl users from harmful or abusive communication.

The research was commissioned in the autumn of 2024 with the express aim of generating insights that would inform NSPCC's response to Ofcom's consultation on the guidance to providers on ways to address content and activity that disproportionately affects women and girls.[14]It is worth noting that this research is one of several that have explored safety-by-design solutions to mitigate Online Violence against Women and Girls (VAWG).[15,16,17] Together, these offer a rich source of recommendations for design changes that would make girls safer. The findings are also intended for broader use by the NSPCC in advocating for stronger online regulation and the prevention and mitigation of online risks to children.

## Research approach

An innovative approach was used to meet the aims of the research. The study mapped out a girl's 'typical' user journey in setting up an online service account and using a service; it then explored what potential each of the design features she encounters on that journey might have to enable or facilitate her being harmed.

Evaluating whether a digital product or feature holds the potential for harm to its users is sometimes referred to as 'abusability testing'. This kind of testing has been used to investigate, among other things, how vulnerable digital authentication mechanisms[18] and Internet-of-Things devices[19] are to causing harm. Abusability testing has been recommended by Ofcom to service providers as a way of pre-empting and limiting misuse of their products, with the aim of creating safer environments for women, girls and other users at heightened risks of online harm.[20]

### Scope and limitations of the research

While this research in intended to contribute to the evidence base around Online VAWG, its focus is exclusively on **teenage girls** who use popular online platforms. That said, many of the risky design features identified by the research also pose risks to younger girls, and to children more broadly regardless of their sex or gender identity, and several might theoretically pose risks to adult women.

The research explored a variety of design features that children interact with in their daily lives. Of specific interest were design features in **user-to-user services** that are subject to regulation under the Online Safety Act and are popular with children. Search services were out of scope, as were user-to-user services that are unlikely to be accessed by children.

The study considers how design features can facilitate a particular type of risk to girls: **online contact risks**[21] **or abusive online communication**. For the purposes of this research, online contact risks include, but are not limited to, sexual harassment, sexual solicitation, intimate image abuse, technology-assisted child sexual abuse, bullying, threats, extortion and hate speech. The study is primarily concerned with abusive communication that girls receive or that is specifically directed at girls, rather than any abusive communication that they may see while online. This is recognised as a limitation of the study, as evidence suggests it is common for girls to see sexist comments and jokes or hate speech exchanged between other service users, and that girls consider their exposure to such content to be harmful. Other types of online harm that do not fall under the umbrella of online contact risks – such as exposure to harmful[22] content or commercial risks – were considered out of scope.

More specifically, the study focuses on online communication abuse perpetrated **by strangers**. Children and young people have various understandings of the term 'stranger';[23] for the purposes of this research, the term refers to users who are not known to the girl who is victimised, even if those users feel familiar to her because she has interacted with them online or because they have mutual real-life acquaintances or online connections. Girls can, of course, be abused online by people they know in real life: their schoolmates, for example, might bully them online as well as at school,[24]while intimate partners may carry out abusive image-sharing behaviours online alongside other forms of domestic abuse committed in person.[25] The reason this research focuses on strangers is not

because they are necessarily more likely to direct abusive communication at girls compared with girls' acquaintances, peers, or family members (although there are indications this may be true,[26] especially in the case of the offence of 'sexual communication with a child'[27]). Instead, it is because strangers in the online world add another layer of risk, over and above the risks posed by people who girls know or encounter in real life. This study explores how design features offer opportunities for contact between girls and individuals to whom they would not ordinarily be exposed in offline settings. It explores how platforms – by virtue of their design features – enable complete strangers to infer a girl's gender and potential vulnerabilities, and to direct abusive communication towards her.

For the most part, this research treats girls who use online services as if they were a single undifferentiated category of user. This is a limitation of the research, given that girls' vulnerabilities are often intersectional. Evidence suggests that girls from LGBTQ+ and ethnic minority backgrounds are more likely to have strangers among their online contacts[28] and may, therefore, be at higher risk. There are also indications that the prevalence of online harm varies by girls' age, by whether they are in receipt of free school meals[29] and whether they have other protected characteristics or additional vulnerabilities.[30] This research does not explicitly set out to identify how platform design features might aggravate the risk of abusive online communication for girls with additional protected characteristics; but, where this was considered a possibility by the researchers, it was noted in this report.

## Methodology

The research was carried out between November 2024 and January 2025 and involved workflow mapping and practical experimentation on 10 platforms, supplemented by desk research and interviews with subject matter experts.

### Selecting platforms to investigate

In order to cover a wide variety of design features, 10 platforms were selected for investigation. All are user-to-user services that are subject to regulation under the Online Safety Act. The sample was primarily designed to be wide-ranging in terms of function: it consists of video-sharing, social media, gaming, gaming-adjacent, and messaging services. Most platforms are well established and popular with children in the UK, including girls – with the five platforms that have the highest usage rates in the UK population of 3–17 year olds among the selection.[31] Two that currently have lower reach among children in the UK were included to expand the variety of functions: one is a social media discovery app aimed at helping users meet and chat with new people, the other an app to search for and post images as a form of self-expression and exploration.

An account was created on each of the 10 platforms for a fictitious 14-year-old girl. Where age or date of birth was requested, it was made clear to the platform that the fictitious user was 14. None of the accounts were linked to parent or family accounts, meaning that parental controls were not applied.

### Mapping platform workflows

The fictitious girl user was used by the researchers as a device for exploring the platforms. They systematically recorded and visually mapped the following for each of the platforms:

- The registration process: including what information the girl user was required to submit, what optional information was requested and how the request was presented to her, what guidance was offered to the user about what personal information she should enter or link to, and what personal or identifying information the platform permitted the user to enter.
- Editing of user details: including what additional personal or identifying information was requested after registration, and what the girl user was encouraged and allowed to submit.
- Activity and engagement: including what options the girl user was given to search or discover other users, connect with others, and interact with them and what options she had to create, curate or find content.
- Visibility controls: including settings for privacy, discoverability, and interactions with others, and for the types of content the girl user could see. All default settings were noted, as was the ability to adjust settings and the options available.

The 10 workflow maps[32] provided a visual summary of all the potential risk points in a girl user's journey through the 10 services.

### Desk research and practical experimentation

To determine which of the features captured by the mapping exercise had the most potential to be abused, it was necessary to understand the typical sorts of tactics perpetrators use to commit online communication abuse. The researchers carried out a non-systematic scan of grey and academic literature published since 2000 to establish, in broad terms, what is known about the online victimisation of girls and the behaviours and motivations of those who send online abusive or harmful communication. The review used search terms like 'offender' and 'perpetrator tactics', and covered topics including online grooming, sexual harassment, and online hate. This resulted in the development of 12 indicative perpetrator archetypes, whose motivations ranged from malicious to naïve. An outline was drawn of the typical ways in which each type of perpetrator approaches their victims, their objective in making contact with a child, and the tactics they use to make or maintain contact and achieve their ends.

The archetypes were not intended as end products of the research, but as tools to inform practical experimentation on the 10 platforms. The researchers used the archetypes, alongside the 10 platform workflows, to visualise how a perpetrator using a platform could commit abuse: could a malicious actor recognise if someone is a girl, identify a user as a potential target, and communicate with their target?

Using fake adult accounts, the researchers systematically explored what information about the 14-year-old fictitious girl was visible to other users, including adults and strangers. They also examined how discoverable she was on the different platforms; whether others could contact her; and whether platforms currently do anything to reduce the possibility of potentially sinister connections or warn child users about potential risks.

### Interviews with subject matter experts

Virtual interviews lasting up to an hour were conducted with eight professionals who have expertise in the design of platforms, on cyber safety and security, or on children's online victimisation and protection. Six were from civil society organisations; one from the technology sector; and one was from the finance sector. Research participants were asked about the interplay between technological design features, on the one hand, and perpetrator tactics or user safety, on the other. Their insight helped to further develop the perpetrator archetypes, to identify design features that pose risks to girls, and to shape the potential solutions outlined in this report.

Several roundtable discussions were also held with PA Consulting staff who have expertise in areas like AI, Digital Identity, Law Enforcement, Intelligence Collection, and Regulation, to develop and sense-check the solutions in this report.

### A note on the use of fake accounts

The use of fake accounts in this research meant that no real children were exposed to safeguarding risks. Since online interaction was restricted to the fake accounts that the researchers had created and were managing, any risk that the researchers would experience abusive communication during the project was kept to a minimum.

The research did not involve observing interactions between the fictitious 14-year-old character and users who were unconnected to this project. The researchers managing the accounts of the fictitious girl did not initiate interaction with real users; on the occasions that the girl's accounts received contact from real users, the researchers did not respond. By taking this approach, the potential for real-world impact on individuals who were not part of the research was kept to a minimum.

The fake adult accounts created to represent malicious actors interacted only with the fictitious girl. Any abusive communication between the girl's accounts and the other fake accounts was carefully staged for experimentation purposes. As part of the testing, abusive communication was sent from the researchers' fake adult accounts to the fictitious girl to test whether it would be blocked or censored by the platform. The text used in the body of the messages was fabricated, but to make it realistic it was based on findings from research about misogynistic communication abuse[33] and online grooming.[34]

All fake accounts were closed at the conclusion of the research exercise. This ensured there was only a small timeframe in which real users could view the profiles of the fictitious girl and adults, or attempt to engage with them, thus minimising the real-world impact of the fake accounts on those who were not connected with the project.

## Structure of this report

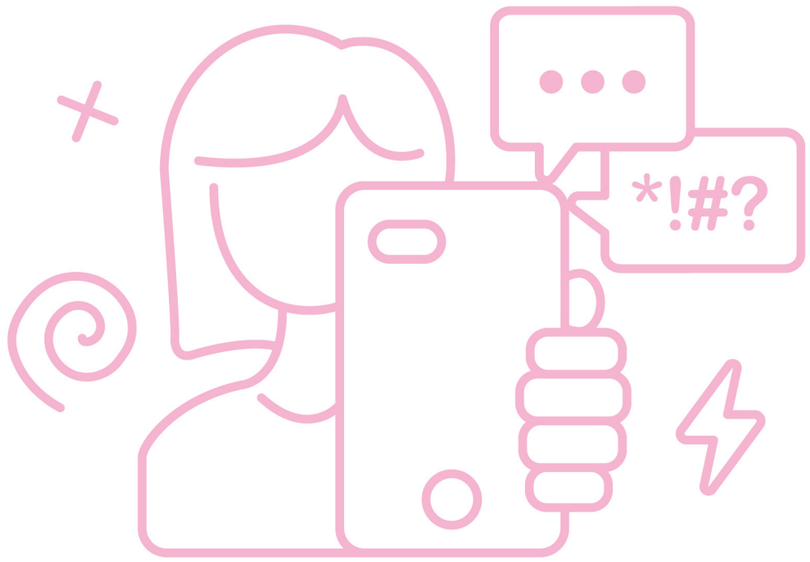
The research identified six areas of design that malicious actors can exploit to identify and target girls with abusive or harmful communication online.

Chapters 2 to 7 present each of those areas in turn, picking out the design features that are particularly risky and suggesting practical solutions that could be put in place by technology companies without affecting platforms' essential functionality. Each chapter includes commentary on how these recommendations supplement and strengthen Ofcom's Illegal Content Codes of Practice, which were published while the research was taking place and came into effect at the time of writing (March 2025).

Chapter 8 takes a step back from specific design features and explains how platform design more generally requires reconsideration. It argues that platforms are currently being built and run on the basis of principles that place minimal weight on children's rights and safety and suggests actions that technology companies can take to make user-to-user services safer for girls to be in and enjoy.

Chapter 9 sets out all 27 of the proposed solutions that could be used to address the risky features uncovered by the study. It also reiterates that there would be less need to implement design fixes retrospectively if child-centred design principles were adopted from the outset and applied throughout the development of digital products that children are likely to use.

Finally, Chapter 10 outlines NSPCC's recommendations from the research to Ofcom, the UK Government, the technology sector and to those researching online VAWG.






# 2 Risky design area: Online Profiles

When registering to each of the 10 user-to-user services that form the focus of this study, a new user is required to provide information about themselves that may relate to name, email, age, or location. This information forms the basis of the user's online profile, a version of which is visible to other users and can be used to find, connect and interact with them.

Once registered, a new user is able to add further information or edit the information they have given to the platform. Editing an online profile typically involves navigating to a profile settings page and updating information like a profile picture, bio, age, interests, and public posts, or customising their avatar. Users can sometimes choose the visibility of these elements, making them public, private, or accessible to selected connections, depending on the platform's privacy settings.

## 2.1 What is the purpose of this feature?

Users create or curate profiles to express identity, attract followers, connect with others, or present a professional image. For platforms, user profiles enhance engagement by encouraging personalisation, attracting new users through appealing profiles, and supporting social discovery. Additionally, detailed profiles provide data that platforms can use to improve algorithms, tailor content recommendations, and offer targeted advertising.

## 2.2 Why is this feature particularly risky?

Sharing information through an online profile can assist malicious actors to identify users who fit their criteria as prospective victims. The more information that a platform asks for, allows a girl user to enter, and then makes visible to other users, the more likely it is that a malicious actor would be able to recognise that she is young, female, and possibly has other characteristics that make her a desirable target for abusive communication.

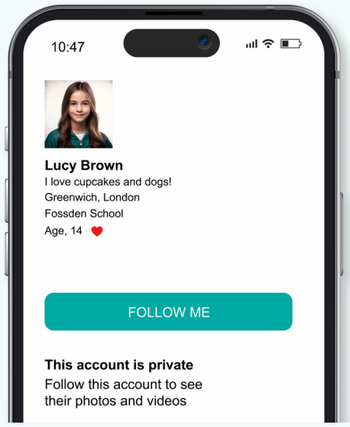
Most platforms in this research allowed the addition of personally identifiable information in a profile, whether as a display name, a username, or as part of a bio. There was often no guidance to users as to what information they should avoid sharing, and no restrictions to what a girl user could potentially add about herself, including full name, gender or pronouns, school name, age, location, and information that reveals her circumstances and her likes and dislikes. Profile pictures normally consisted of a photographic self-portrait ('selfie') of the user; this usually makes apparent whether a user is a girl and can potentially disclose her ethnicity, religion, or visible disabilities. Elsewhere, profile pictures consisted of avatars that were gendered and could be customised to show additional information about the girl user, including her skin tone, her taste in clothes, and symbols of her identity; these could sometimes be customised in sexualised ways that other users might interpret as indicating the user's sexual availability.

At least some of this information is visible to other users who are strangers to the girl. Even if an account is set to 'private', other users can see, at the very least, the user's profile picture and username – these are normally sufficient to identify her as a girl. Some platforms allow even more information to be visible, including her bio, the number of connections she has, who she follows, or what content she has 'favourited', which can potentially reveal her vulnerabilities or be used as intelligence by a perpetrator to create trust with a prospective victim (see Box 2.1).

As there is normally no guidance as to what information to share, users tend to follow the social norms that they see on the platform, potentially revealing more about themselves than they need to (see Box 2.2).

Most platforms nudged users to add extra information about themselves on an optional basis, while at the same time using enticements or 'dark patterns' to encourage compliance (see Box 2.3).

Children, particularly younger children, often underestimate the level of online risk involved in sharing information about themselves.[35] While online safety organisations offer children and their parents advice about setting up profiles without sharing unnecessary information, platforms could do more in this regard. For example, almost none of the platforms in this study gave users the option to see what their online profile looked like from the perspective of a stranger, to help them understand that their profile could be revealing and amenable to exploitation.




## Box 2.1 Research insights

On **Platform A**, users are invited to add a bio. This is visible to all users, including unconnected users, even if the default 'private account' setting is on.

Users are given no direction as to what they should or should not include in their bio and are therefore influenced by platform norms. There was no restriction on what could be added in a bio, and nothing to prevent a girl user from displaying her full name, location, school, or age.



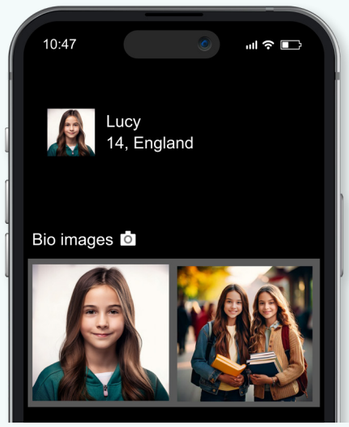

## Box 2.2 Research insights

On **Platform B**, it is common practice for users to introduce themselves to others who use that space by providing a lot of information about themselves. This can often include information relating to likes, dislikes, and particular vulnerabilities. A new girl user may feel social pressure to follow this norm.

Notably, there did not appear to be any checks or restrictions on the display name a user could choose. Malicious actors could potentially use overtly misogynistic names. There was nothing to stop a girl user from using her full name or from including a year of birth or location as part of her display name.






## Box 2.3 Research insights

On **Platform C**, child users are encouraged to add additional photos of themselves (in addition to the one required at registration) to unlock access to other user's additional photos – this tactic is generally recognised as a dark pattern or dark design.

In summary, this research identified four particularly risky features related to online profiles:

1. **The permanent visibility of basic identifiable information,** such as profile photos, bios, or usernames, to all other platform users. This facilitates malicious actors to recognise when a user is a girl and deduce other intersectional characteristics that may make her a desirable target of abuse.
2. The **unrestricted ability to edit bios to include personal identifiable information**, including full name, age, gender, location, and school. Sharing these types of information leaves vulnerable users exposed to manipulation by malicious actors who, according to the subject experts who were interviewed for this research, may use these details to tailor their abuse or grooming to be more effective.
3. The **availability of highly gendered avatars**, including their apparel and customisation, which increases the ease with which other users can identify someone as young and female and target them.
4. The lack of settings to **configure the presentation of curated content** to other users. Without this level of control over what specific elements of their profile are visible to others, users cannot finetune which aspects of their privacy to preserve. If users are only given a crude choice of either making everything visible, or nothing visible, they may accept full exposure to other users, making themselves vulnerable to malicious actors.

## 2.3 Proposed changes to feature

| | Potential solution | Description |
|---|---|---|
| 1 | Introduce public-facing anonymous avatars | Set a non-gendered avatar as the default image for a child's account when viewed by users the child is not connected with. This would be separate to the profile picture or avatar presented to users they are connected to. The latter would only become visible after a connection has been made. |
| 2 | Automatically detect personally identifiable information in free-text bios | Use AI or other technological tools to detect and block the input of personally identifiable information in profile bios. This could also be an opportunity to offer users supportive education as to why inputting this type of information is risky and has been prohibited. |
| 3 | Restrict the type of customisation available to young children for avatars or in-game items | Limit young child users from obtaining overly sexualised or other content inappropriate for young children for use in their own personal avatars, including body shape, facial features, hair, clothing, and handheld items. Children should be informed as to why certain items are unavailable for them to purchase or wear in their in-game avatar. |
| 4 | Remove dark design patterns that encourage users to upload more information to access more of the platform | Remove features or prompts that subtly encourage child users to upload more of their own information (for example, bio, photos, stories, age) to access additional parts of the platform's functionality. This includes examples where users are prompted to upload additional 'selfies' in order to see other people's additional 'selfies'. |
| 5 | Increase the configuration of settings for presenting curated content to other users | Introduce new settings at an individual media level so that a user can decide whether or not individual videos, photos, and posts are shown to others. This would be complimentary to the blanket setting that most platforms currently offer. |
| 6 | Ability to view your own profile from another user's perspective, and reminders to do so | Provide the user with the ability to view their own profile from the perspective of specific groups of users (for example, users they are not connected to) to help understand their privacy and online presentation. This would include periodic nudging to encourage users to perform this check. |

### Commentary on Ofcom's Illegal Content Codes of Practice

While Ofcom recognised the dangers associated with online profiles in their draft illegal codes consultation (November 2023),[37] there is nothing in the final published illegal codes that directly addresses the risks identified in this research. The six solutions presented above would strengthen the safeguarding of children, including girls. They would also supplement measure ICU F2: Support for child users, expanding the points at which a child is provided with supportive information and allowing girls to make more informed choices about the information they allow other users to see.



# 3 Risky design area: Searching for other users

Users of the 10 platforms studied in this research are able to search for other users online. A user can do this by inputting names, usernames, or keywords in a search bar; by exploring connection lists of friends or mutual contacts; by responding to automated suggestions like 'People You May Know' or 'Suggested Contacts'; by syncing a phone book to find contacts; or by reviewing interaction-based lists such as 'Recently Played With' on gaming platforms.

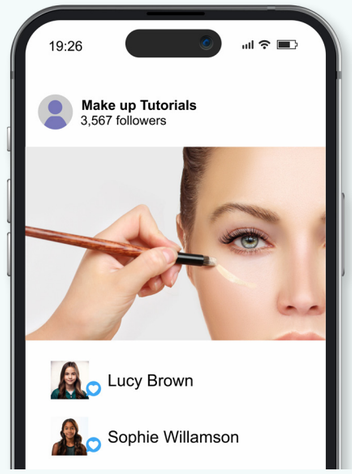
## 3.1 What is the purpose of this feature?

Users use Search functions to reconnect with acquaintances, expand their networks, discover like-minded individuals, or follow influencers and professionals of interest. For platforms, these mechanisms drive engagement, promote network growth, and engender loyalty to a platform by fostering interconnected communities, while also generating valuable relational and behavioural data that can enhance algorithms, personalisation, and monetisation strategies.

## 3.2 Why is this feature particularly risky?

The ability to search for and find other users on a platform presents malicious actors with a continuous stream of potential victims that match their specific preferences.

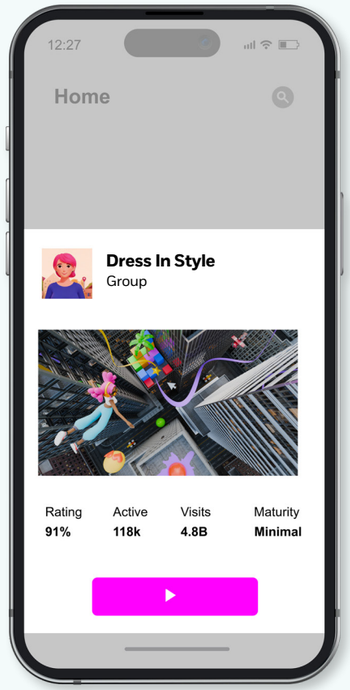
In this study, the researchers were able to discover the profile of the 14-year-old fictitious girl – even though they were registered as adult users – simply by searching for common first names for girls. They could find other girl users by searching through 'community member lists' associated with stereotypical 'girl' interests: they could then deduce when someone in their search results was a girl by looking at their profile picture, gendered avatar, or username; from information in their bios; or through the content that they had made visible to other users (see Box 3.1). By searching through LGBTQ+ or mental health communities, they found girl users who had additional vulnerabilities. Having found one girl user, they were then able to find others by looking at the profiles of users who had 'liked' that girl's posts or users on her connection list.




### Box 3.1 Research insights

On **Platform D**, adult users can search for communities likely to be frequented by girls based on stereotypical 'girl' interests. They can then review who has engaged with content in that community and go on to add or communicate with girl users of interest to them.

This includes communities where they are likely to find particularly vulnerable girls, such as mental health communities.

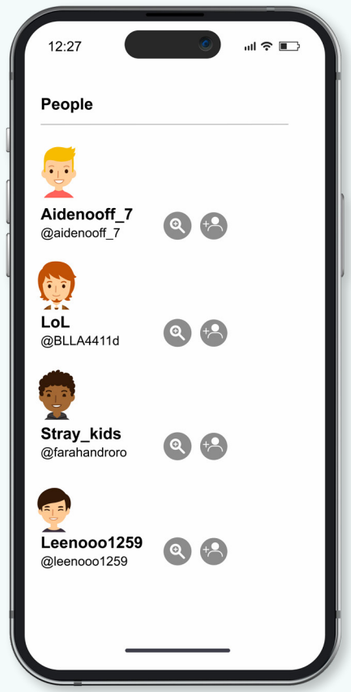



### Box 3.2 Research insights

On **Platform E**, adult users can search for and join games that girl users are likely to frequent based on stereotypical girl interests.

**Platform E** provides lists of all the users the adult had recently played with (right image). The list includes child users, allowing the adult user to find and add them in a frictionless procedure.

Search results also show who is currently online. This means that a stranger can potentially gain immediate access to a prospective victim.




An alternative way of finding girl users is by playing games that are popular with girls, and then searching through 'recently played with' lists for the profiles of other players that had taken part in the game (see Box 3.2). In their interviews, subject matter experts described how perpetrators might also exploit network algorithms to find prospective victims for them: if a perpetrator tailors their own online profile to give themselves the characteristics they are interested in targeting, and then engages with spaces frequented by children, they can wait for the algorithm to present them with suggestions for contacts or 'People you may know' who have similar characteristics (for example. age, interests, location).

In summary, this research found three particularly risky features related to Search functionalities:

1. The ability for **adult users to see child users in their search results**. This provides an efficient tool for malicious actors to access children.
2. **Children being recommended to adults as suggested contacts** based on algorithms, serving potential victims to adult abusers, often tailored to meet an abuser's victim-type.
3. The ability to **view a child's list of connections**. Research participants noted that this is used to provide malicious actors with intelligence to increase the success of manipulative tactics or increase their pool of potential victims.

As discussed later in this chapter, the second and third of these risks are addressed by Ofcom's Illegal Content Codes of Practice. The proposed solutions set out in section 3.3, therefore, do not cover these two risks.

## 3.3 Proposed changes to feature

| | Potential solution | Description |
|---|---|---|
| 1 | Prevent children from appearing in the search results of adult users (unless the child's username precisely matches the 'search term' used by the adult). | No longer include children in search results when searched by any adult user. The only exception would be if the adult uses a precise username to search for a specific child. To be effective, this solution needs to be implemented in conjunction with a robust age assurance strategy. |
| 2 | Prevent children from being displayed in 'recently played with' lists or 'community member' lists. | Hide children from lists that facilitate connections from strangers, including 'recently played with' lists on gaming platforms or 'community member' lists on large community pages on social media platforms. |
| 3 | Hide child interactions with content | Remove detailed information of what content a child user has interacted with. Give an aggregate count (for example, "11 likes") with no ability for users other than the poster to break this detail down further and see who those 11 users are. |

### Commentary on Ofcom's Illegal Content Codes of Practice

Ofcom has recommended through their Illegal Codes that child users should not appear in other users' connection lists; that child users should not be suggested as potential connections in other users' connection or network expansion prompts; and that children's connection lists should not be visible to other users. These measures will make it harder for malicious actors to search for and find children with some of the methods that the researchers used in this study.

The three additional solutions above would add further mitigations. By ensuring that child users cannot be found by adults in any search results – even using novel methods, such as 'recently played with' lists – girls would be shielded from unnecessary exposure to strangers who may want to target them with abusive communication. Arguably, this restriction is needed even in temporary gameplay set-up situations, to prevent perpetrators who frequent gaming environments where children are likely to play from finding and accessing girls.

# 4 Risky design area: Connecting with others

Once a user has searched for and found a user who they want to interact with, or has received an algorithmic recommendation for another user, many platforms allow them to create a formal online connection. The user who wishes to initiate interaction is usually able to send a connection request to the person they want to 'friend' or 'follow'. Users of messaging platforms can add someone they are already connected to into the membership of a group chat, often without needing to request their permission: the person they have added would then immediately be connected with multiple other users, some of whom may be strangers to them.

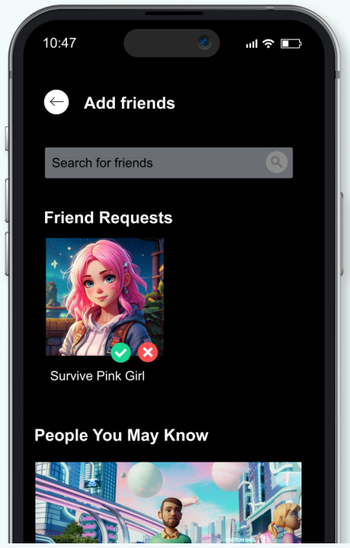
## 4.1 What is the purpose of this feature?

Users engage in these connections to build relationships, share interests, gain visibility, or access content and updates from individuals or organisations they value. For the user, this fosters a sense of community, networking opportunities, and tailored content. Platforms benefit by increasing user engagement, retention, and data generation, which enhance targeted advertising and drive revenue while expanding the network effect that makes the platform more attractive to additional users.

## 4.2 Why is this feature particularly risky?

Malicious actors can exploit connection functionalities to make an approach, initiate a dialogue, or begin a relationship with a prospective victim. These are significant early steps to grooming a girl or sending her abusive communication.

The platforms in this study mostly had straightforward, frictionless ways of connecting users. Some of them facilitated connection between adult and child users. The researchers in this study (who had adult accounts) were able to request a connection with the 14-year-old fictitious girl on several platforms (see Box 4.1).




### Box 4.1 Research insights

On **Platform F**, adult users can add child users without restriction.

From the child's perspective, there are no warning prompts to suggest the child might not know this person or that they are an adult.

From the adult user's perspective, once a child user has been added, **Platform F** continued to recommend other similar users as potential connections – many of whom appeared to be child users.

Child users were also recommended adults to connect to: at the point of registering to some of the platforms, the 14-year-old girl user was asked for permission to import her phone contacts and email addresses and encouraged to connect with the owners of those phone numbers and email addresses, even if they were adults.

The 10 platforms generally encouraged users to make connections with other users, using either overt or subtle methods. Many platforms displayed users' friend or follower counts, which quantify users' popularity (to themselves and to other users), and can motivate child users to accept connection requests in a bid to appear more popular. Some deployed 'dark patterns': for example, the option to accept a request was made visually prominent while the option to decline relatively obscure; or positive visual cues and language were used to commend users when they accepted a request. Some displayed 'mutual friends' between the requester and the person invited to connect with them, to signal that the requester was not completely unknown and could be trusted as a connection. Using the term 'mutual friends' to refer to mutual connections is itself liable to create a false sense of security for child users, who may infer that a stranger is trustworthy, like a friend, simply by virtue of having a connection in common.

These design techniques can be successful in persuading children to accept and initiate connections with strangers. Research suggests that over a third of 10–15-year-olds have accepted a friend request from someone they have never met in person, and around a third of 11–18-year-olds say they would be influenced in their decision to accept a friend request or reply to a message from someone based on their mutual friends online. Experts interviewed for this study indicated that perpetrators could exploit the 'mutual friends' feature to create a sense of trust with a prospective victim, increasing the likelihood of the child accepting their connection request.

Once two users have a formal connection, there are worryingly few safeguards in place to protect them during their further interaction. In their interviews, technology experts highlighted a significant flaw in the design principles employed across online platforms – namely, the assumption that a user's connections are inherently trustworthy. This fails to acknowledge that children can make connections expediently, without much thought, and on the basis of a false sense of trust (for example, engendered through mutual connections). It also does not mirror social relationships in the physical world where trust is built over time and constantly assessed.

In summary, this research found five particularly risky design features associated with connecting with others:

1. The **ability of adults to send connection requests to child users**. This can facilitate direct communication between malicious actors and their prospective victims.
2. **Adults being recommended to children as potential connections** during registration, when phone contact lists or email contact addresses are imported from a user's device. This can facilitate contact between children and others whom they were in contact with in the past but may have no ongoing trusting relationship with, and who may be adults.
3. The display of **mutual connections** at the point of accepting or rejecting connection requests. This was raised in multiple interviews with experts as a method that malicious actors employ to engender trust.
4. The ability to be **added or invited to group chats by others**, without permission and with little indication of the group's subject matter or membership. Large chat groups, which can contain a mix of adult and child members who are not known to each other, give considerable scope to malicious actors to approach and communicate with prospective victims.
5. The **reduction in visible safeguards** after the point at which a formal connection has been made between users. This removes protections for children against people who may, in fact, effectively be strangers to them.

As mentioned in Section 1.3 and in Chapter 3, Ofcom's Illegal Content Codes of Practice direct services not to display child users' connection lists to other users, and not to show children in other users' connection lists. In practice, this will mean that neither the sender of a connection request nor the receiver will be aware of their mutual connections once the Codes are in effect. These measures, if combined with a ban on displaying a numerical count of mutual connections to either party, will effectively remove the third of the risks listed above. It is worth noting that the removal of the 'mutual connections' functionality has a downside in young people's own estimation, in that it limits their ability to assess whether to accept a new connection request and to validate the requester's identity. Some of the experts consulted for this research suggested developing a more intelligent presentation of the strength of mutual connections (based, for example, on number of mutual connections that both parties frequently contact) as an alternative to removing the functionality altogether.

## 4.3 Proposed changes to feature

| | Potential solution | Description |
|---|---|---|
| 1 | Prevent adults from requesting to connect with children | Remove the ability for adults to send connection requests to child accounts, meaning it must always be the child user who initiates a potential connection. This should be coupled with an effective age assurance strategy, to reliably distinguish adult users from child users. |
| 2 | Remove the functionality that allows a child to import phone contacts or email contact addresses from their device | Remove the ability for child users to request connections with anyone they already have contact details for stored on their device (this is often one of the first steps when registering with a new platform). |
| 3 | Provide additional descriptions of chat groups | Increase the transparency of likely topics of discussion in messaging groups, so that child users can assess whether to join or stay in a group they have been added or invited to. Create automated tags or flags for groups that are likely to contain misogynistic, sexual, or other content that is inappropriate for children, based on previous messages or shared media within that group. |
| 4 | Increase opportunities to decline and make it easier to decline connection requests | Platform design is currently focused on encouraging users to increase their networks, including nudging 'recommended friends' or intensely positive narrative upon connecting. There should be equal weighting given to design elements that allow a user to reject a connection to those that allow them to connect (for example, accept/reject buttons). This could also include virtual 'holding rooms' (for example, 'suspicious connection requests') for requests from users where the rationale for forming a connection is weak or unclear, such as based only on common location or on similar age. |
| 5 | Implement a 'cooling off' period once connection is made between users | Once two users formally connect, designate a period when there are enhanced restrictions between users. During that period, there would be limitations around the types of interaction permitted between the two users (for example, sending media) and limited visibility of content that the users have posted or curated. |

### Commentary on Ofcom's Illegal Content Codes of Practice

Ofcom's Illegal Codes will help reduce the ability of strangers to connect with child users. Removing the 'mutual connection' functionality will decrease the risk of a girl user assuming a perpetrator is trustworthy because they have connections in common. It will also prevent malicious actors using the 'friend' lists of girls with whom they are connected to identify more girls to target.

As this study has shown, connections between strangers and girl users will nevertheless remain possible, facilitated by the design features described above. Solutions 1 and 2 can work alongside the Codes to reduce opportunities for potentially risky connections; solutions 3 and 4 can empower girls to make informed choices as to whether to enter and stay in a group chat, and to decline connection requests from other users if they wish. Solution 5 removes the assumption that girls' connections are necessarily trustworthy and offers safeguards to girls after, as well as before, they make a formal connection with another user. Altogether, these measures can help to prevent connections being formed or maintained that could enable strangers to communicate abusively with girls.



# 5 Risky design area: Direct messaging

Direct messaging on common online platforms typically involves selecting a contact, typing a message in a chat interface, and sending it, often with options to include media like images, videos, or links.

## 5.1 What is the purpose of this feature?

Users engage in messaging to communicate privately, share information, collaborate in real time, or maintain personal and professional relationships. This functionality offers users convenience, immediacy, and a secure channel for interaction. For platforms, direct messaging increases user activity, enhances engagement, and encourages longer session times, which supports advertising revenue, premium features (like encryption or message customisation), and loyalty by integrating the platform into users' daily communication habits.

## 5.2 Why is this feature particularly risky?

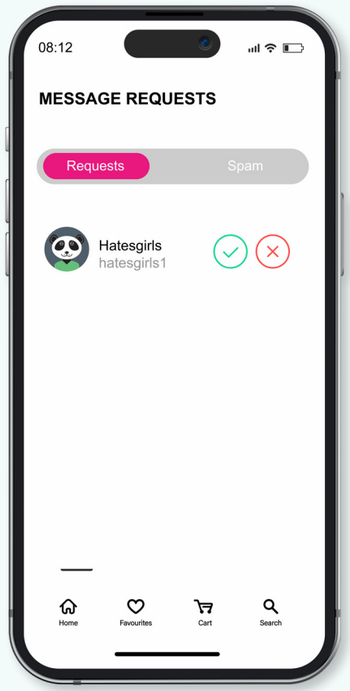
Direct messaging allows users to send or exchange messages in a private environment, where both the interaction and the content of the messages remains exclusive to sender and receiver. Malicious actors can exploit direct messaging to send abusive or inappropriate communication to their prospective victims away from public view. Interaction in private environments can also create a sense of intimacy – as reflected in the language used in many games, where direct messages are described as 'whispers' (/w <text>) – enhancing the potential for malicious actors to develop trust and foster secrecy in order to groom girls.

Content warning: The graphics in this chapter contain explicit language and fabricated scripts. They are designed to represent realistic examples of abusive and inappropriate communication that a girl may receive.

Several of the platforms in this study allowed the researchers (who had fake adult accounts) to directly message the fictitious character registered as a 14-year-old girl. In some cases, the ability to send a direct message did not require a connection between the users; where this was the case, the recipient was normally offered some level of protection from potential abuse by the platform, such as the ability to preview the content of the sent message, the blurring of sent images (to allow blocking or reporting the sender without ever seeing the image), or the hashing out of abusive language in the body of the message. Practical experimentation by the researchers showed that these protective measures were far from infallible: for example, a girl receiving a preview of a message that contains abusive language would still be able to see the abusive language in the preview (see Box 5.1), and filtering misses out various types of profanity and misogynistic hate speech. The protective measures were also not comprehensively applied: one gaming platform did not extend those protections to specific playing contexts, allowing users to receive abusive texts from other players on an in-game phone.

In other cases, users had to be connected before a direct message could be received. Where users were connected, there was often little by way of protection from abusive communication. An adult user connected to the fictitious girl could chat freely with her, send her images, and ask for her email address, telephone number or social media handles to move the conversation into more private forums (a process known as 'offboarding', which research participants warned was a common tactic across multiple perpetrator archetypes). Just one platform in this study used automated filtering to block the girl user from entering her contact details (see Box 5.2).

None of the platforms publicly report that they block the sending or receiving of newly created nude or sexual images, despite the fact that cyberflashing is now well established as a widespread form of harassment of girls. Only some of the platforms investigated here publicly report using proactive technology to detect grooming language or known child sexual abuse images in direct messages (see Box 5.3); where they do, it is only applied in parts of the platform that are not end-to-end encrypted. Altogether, this exposes girls to considerable risk of receiving abusive or harmful online communication.

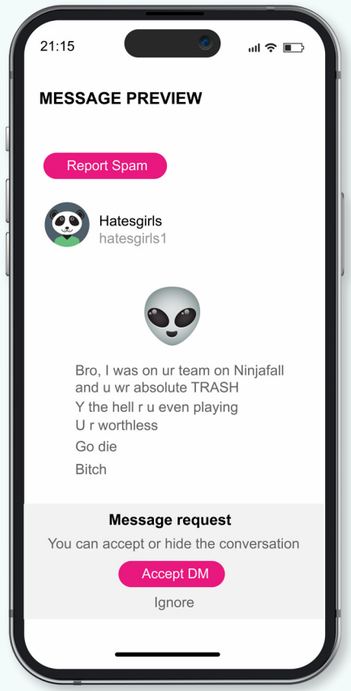


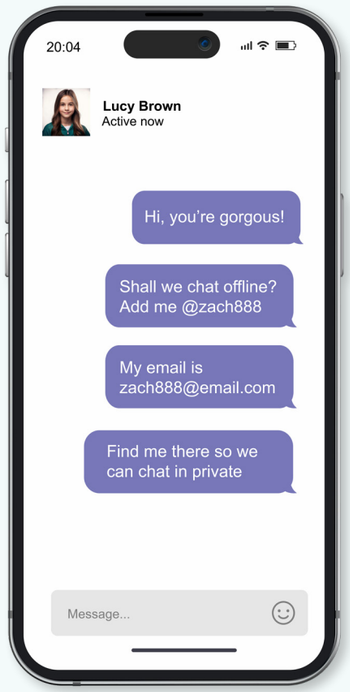

## Box 5.1 Research insights

On **Platform G**, adult users are able to send direct messages to child users who are on the same server even before they are connected.

When this happens, **Platform G** provides a Message Preview. In this case, the Preview was ineffective at preventing the child user from being exposed to harmful communication. It did not warn the child user that the message contained abusive language.

The options to 'Accept DM' or 'Ignore' are visually biased towards accepting. 'Report Spam' is the only other option. The user would need to navigate elsewhere on the platform in order to 'Report Abuse'.

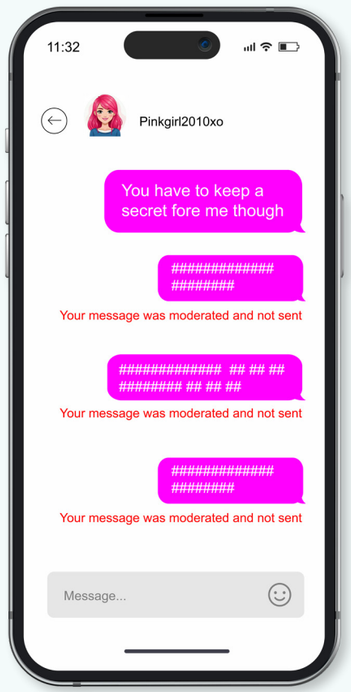


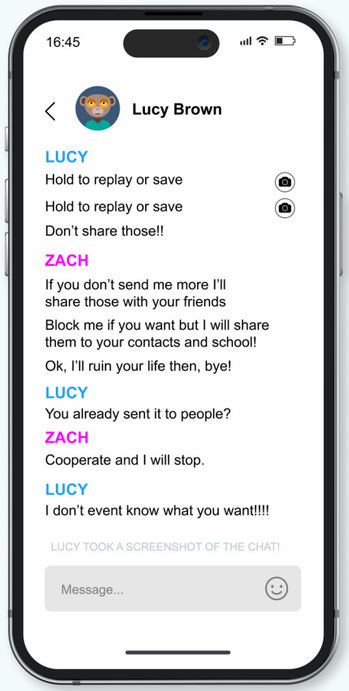




## Box 5.2 Research insights

On **Platform H**, (left image), adult users can freely chat with a child user once they are connected. This includes requesting contact details for offboarding onto more private forums.

By contrast, **Platform I** (right image) blocks or hides these types of requests.




## Box 5.3 Research insights

On **Platform J**, adult users can freely communicate with a child user once they are connected. There was no indication of automated detection being deployed that could identify grooming language or extortion scripts.

While the adult user can use technology to screen record conversations, images, and videos with impunity, if the child user tries to screenshot a disappearing message as evidence of her abuse, the platform notifies the perpetrator. Notifications may dissuade her from reporting her abuse for fear of alerting her abuser.

The researchers also noted that some platforms sent notification to users if their sent message was screenshotted. While this can be a protective measure (preventing private or ephemeral messages from being distributed beyond their intended recipient), it might also inadvertently dissuade victims of online contact abuse from taking screenshots to evidence and report their abuse, as doing so would automatically notify their abuser.

In summary, this research identified three elements of direct messaging that are particularly risky:

1. The ability to **send or receive direct messages between adults and children** without limitations, restrictions, or user-definition. Being able to communicate directly, freely and in private enables malicious actors to have immediate access to prospective victims, gives them a direct channel to deliver abusive communication, and allows them to develop intimate grooming relationships outside of public scrutiny.

2. The ability to **send abusive or inappropriate content (media and text) without detection, prompts, blurring, or blocking**. Experts interviewed for this study indicated that the technology for this does exist but is sporadically employed across platforms, leaving users exposed to harmful contact with little in place to prevent it.

3. The ability to **send contact details through direct messages**, which facilitates offboarding onto more private platforms and cross-platform risk and reduces the chance of intervention by third parties.

As mentioned in Section 1.3, Ofcom's Illegal Codes recommend that platforms should no longer allow direct messaging between unconnected users. They additionally recommend that child users should be given the chance to actively confirm that they want to receive a message from someone they are not connected with on services that do not have user connection functionality. These provisions will, to some extent, reduce the first of the risks, but still leave child users vulnerable to online contact risks from users they are formally connected to.

## 5.3 Proposed changes to feature

| | Potential solution | Description |
|---|---|---|
| 1 | Block adults from direct messaging children, unless a child has signalled that the user is trusted | Require children to select which specific adults are considered trusted by adding them to a 'family and friends' pool in their account settings. Direct messages from other adults would be blocked (on services with connection functionality) or would need to be explicitly accepted by the child user (on services without direct connection functionality). This should be coupled with an effective age assurance strategy, to reliably distinguish adult users from child users. |
| 2 | Blur or hide direct messages between users who have recently formed a connection | When a child user forms a new connection with another user, prevent the content of messages sent to them from being visible and flag messages with automated content descriptions (for example, 'this message may contain nudity') until the child user has made a decision as to whether to accept receipt. This should be implemented in conjunction with the recommendation in Ofcom's Illegal Codes to provide supportive information to child users at the point when they receive their first direct communication from a user. |
| 3 | Automatically detect and block inappropriate or offensive direct messages | Use automated tools to detect, block, and remove inappropriate or offensive messages between users, including nude or gore images or explicit text. This measure should be applied across the board where child users are concerned, regardless of whether or not the users are connected. |
| 4 | Automatically detect messages that relate to offboarding or sharing of contact details | Use automated tools to detect phone numbers, email addresses, and social media handles, or language that indicates that a user is requesting to shift interaction with another user onto other, more private or unmoderated environments. Prevent these messages from being sent to child users or, at a minimum, provide a warning to users about the risks associated with uploading their contact details. |
| 5 | Integrate screenshot capability into a reporting function | Create an integrated reporting mechanism to facilitate discrete screenshotting of direct messages for safety reporting reasons. The screenshot can only be saved as part of a safety report and, importantly, does not notify the abuser it has been taken. |

### Commentary on Ofcom's Illegal Content Codes of Practice

The inclusion of direct messaging restrictions for children in Ofcom's Illegal Codes will lessen children's risk of receiving abusive communication from strangers. However, it is important to acknowledge that child users often make connections with other users who they barely know or do not know at all, either expediently or based on a few commonalities, and that these connected users are essentially strangers to them who may pose risks to their safety. Direct messaging protections should, therefore, be extended to interactions between connected users.

The solutions above add further direct messaging protections for child users, which can protect girls against online contact risks from people – including adults – who they may or may not be formally connected to. Solution 4 specifically protects against cross-platform risks, while solution 5 facilitates the reporting of abusive experiences. Consideration should also be given to closing loopholes in the protective measures suggested by Ofcom, for instance by extending protections to players who use inter-player communication functionalities built into specific games.



# 6 Risky design area: Livestream and in-game chat

Livestreaming and in-game chat are two types of real-time interaction that allow users to have dynamic and immediate exchanges with other users. Livestreaming typically involves using a platform's tools to capture and broadcast audio, video, and gameplay. In-game chat allows players to communicate while playing – this can take place via text but is commonly through voice, using integrated features like chat boxes or push-to-talk systems.

## 6.1 What is the purpose of this feature?

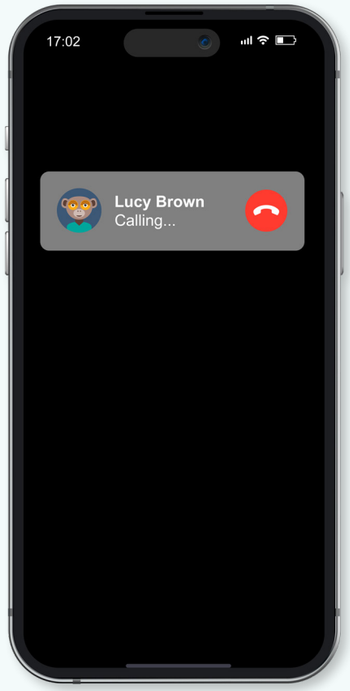
Users engage in these activities to share experiences, build communities, coordinate gameplay, entertain, or receive feedback. For platforms, these features boost user engagement, foster communities, and increase retention. Livestreaming draws audiences, often generating advertising revenue and subscriptions, while in-game chat enhances the social and collaborative aspects of gaming, which keeps users active and attracts new players through word-of-mouth and social connections.

## 6.2 Why is this feature particularly risky?

Real-time online interactions can be fast-moving, involve multiple users, and make use of simultaneous channels of communication – as a result, they are typically extremely challenging to moderate, leaving users of livestreaming and in-game chat vulnerable to abusive communication. Malicious actors can exploit the complexity of these environments to direct abuse at prospective victims, secure in the knowledge that platform moderation is minimal, and emboldened by physical separation from their victims and, in some cases, by group dynamics and the ability to operate anonymously.

The platforms in this study that had livestreaming capabilities permitted adults to interact with child users. The researchers (who had adult accounts) were able to place a video call to the 14-year-old fictitious girl once they were connected with her (see Box 6.1). They could – if they wished – have taken screengrabs and recordings during the call; this enables 'capping', a tactic used by perpetrators of grooming, child sexual exploitation, and sexual coercion to covertly generate child sexual abuse material (CSAM).[43] Some of the platforms allowed child users to broadcast live to large audiences, including to strangers; and, depending on the child user's privacy settings, may permit users to post comments in real time during the child's stream that can be abusive or can potentially be used to manipulate them. Research from 2018 indicated that one-in-10 surveyed pupils aged seven to 16 who reported having video chatted with strangers had been asked to take off or change their clothes on screen; overall, six per cent of pupils with experience of video chatting or livestreaming had received a request like this.[44] While these risks may not be specific to girls, CSAM generated through livestreaming overwhelmingly consists of images of girls.[45]

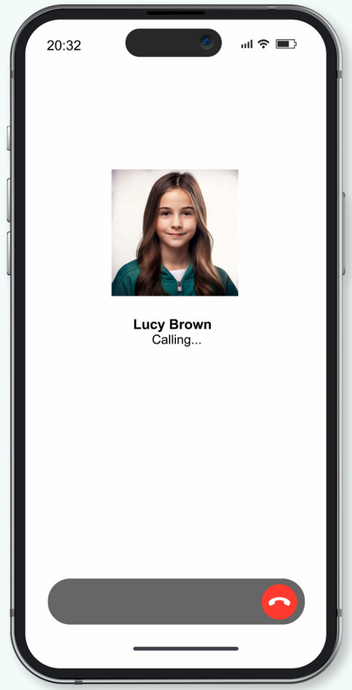
Oversight and protections are especially difficult to implement in gaming environments. These often involve a variety of modes and channels of communication (for example, server text or voice chats, in-game features, and objects like banners or signs) alongside the use of game-adjacent applications. Malicious actors can use their gaming avatars to easily mask their real identity by posing as fictional characters or as peers of the same age. The immersive and interactive nature of gaming, and the trust that develops between players through shared play, lends itself to the relatively easy manipulation of child players by strangers. The researchers in this study were not prevented from communicating with the 14-year-old fictitious girl in various ways during gaming: through voice or text; by 'calling' her gaming avatar using in-game features like phones or radios; by showing written messages to her avatar on customisable signs; or by having their avatar perform actions on hers (see Box 6.2). The easy, frictionless, accessibility of girls to strangers on gaming platforms provides enormous scope for abusive online communication. The pool of prospective girl victims has grown in recent years, with over half of girls engaging in online gaming and around seven-in-10 of those aged 11–18 using in-game chat functions.

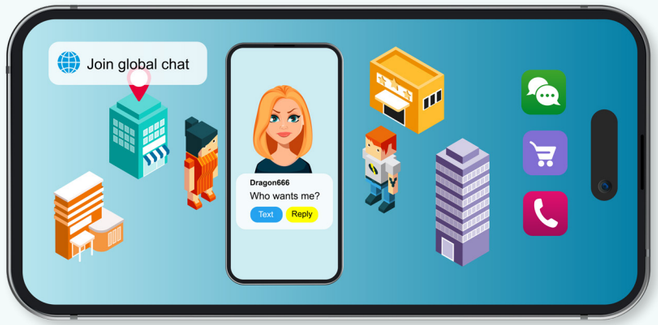



### Box 6.1 Research insights

On **Platform K** (left image) and **Platform L** (right image), adult users were able to video call child users they were connected to.

Video calling can potentially be used as an immediate, intimate, and direct channel for delivering abuse.





### Box 6.2 Research insights

On **Platform M**, direct messaging is limited by default to 'No One'. Despite this, other users can contact child users through in-game features like phones or radios, some of which emulate real-world messaging apps.

Users on **Platform M** can communicate with each other in numerous ways aside from chat and messages. A malicious actor can use customisable signs and available performable actions (for example, grab and kiss) on a girl user's avatar. A misogynistic culture appears to be fairly typical of some games that are age rated as 0+.



In summary, the research identified two features related to these real-times interactions that are particularly risky:

1. The **ability for young children to have live video chats (and livestream)** with other users. Experts that were interviewed for this research described livestreaming as a key tactic used by perpetrators to sexually exploit vulnerable users, using coercion, control, trickery, or aggression.
2. **Under-powered privacy and safety settings** related to in-game chat features, which do not account for the complexities involved in real-time interactions and leave users exposed to abusive communication from other players.

## 6.3 Proposed changes to feature

| | Potential solution | Description |
|---|---|---|
| 1 | Increase the lower age limit for livestreaming | Set suitable age limits for accessing video chat and livestreaming functionality, and highly protective default settings for younger users. This is to account for the high level of risk associated with real time interaction, and the maturity and risk awareness of younger children. |
| 2 | Prevent adults from being able to place live video calls to child users | Require children to select which specific adults are considered trusted by adding them to a 'family and friends' pool in their account settings. While live video calls from these adults would be permitted, video calls from all other adults would be blocked. This should be coupled with an effective age assurance strategy, to reliably distinguish adult users from child users. |
| 3 | Implement use of anti-screen recording technology | Prevent screen recording technology being employed when engaged on parts of platforms where privacy is highlighted as a significant benefit of that feature – utilising technology employed in sectors like finance. |
| 4 | Deploy automated language detection across environments likely to be used by children | Implement automated technologies to identify and block abusive or predatory language in real time interactions between users, including up-to-date variations on common words aimed at bypassing filters (for example, 'corn' instead of 'porn'). |
| 5 | Enable customisation of safety settings for each communication mode in complex multi-user environments | Recognise that many gaming platforms offer a complex variety of methods for communicating with others. Provide users with the ability to limit each of those methods in their user safety settings and set the default for every mode of communication to 'off' for the youngest users, providing education prompts to users when they try to turn them on. |

### Commentary on Ofcom's Illegal Content Codes of Practice

There is a significant gap in protections for children from illegal harms during their real-time online interactions. Ofcom's Illegal Codes do not recommend any protections for children who livestream. They make one recommendation for protecting children in gaming environments, proposing that child users are given the means to actively confirm they want to receive a direct message from another player.

The solutions listed above offer supplementary ideas for protections to children. These are sorely needed to tackle the risk of abusive online communication abuse associated with real-time interaction, and especially in complex, multi-channel, immersive gaming environments.

# 7 Risky design area: Gifting and Rewards

Gifting and rewards on online platforms typically involve selecting a predefined gift (for example, virtual items, currency, cosmetic changes to avatars known as 'skins') or transferring credits through in-platform systems, often facilitated by payment methods or accumulated points.

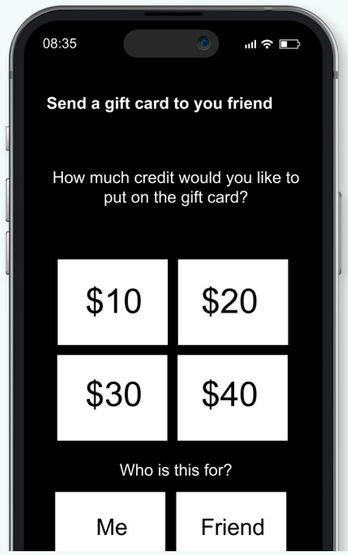
## 7.1 What is the purpose of this feature?

Users might gift or reward others to show appreciation, celebrate milestones, support creators, or foster goodwill within communities. This activity benefits platforms by driving monetisation through purchases of gifts or virtual currencies, increasing user engagement as participants exchange tokens of appreciation, and reinforcing community ties that encourage retention. Additionally, platforms can leverage gifting systems to incentivise spending, highlight premium features, and create a sense of value and reciprocity among users.

## 7.2 Why is this feature particularly risky?

In-game gifting and rewards can be exploited by malicious actors to instil a sense of trust, generosity, and obligation in the receiver. Giving virtual gifts, in-game currency, or valuable items can help malicious actors build rapport and gain the trust of child users,[49] leading to a dependency or sense of indebtedness that can make children more susceptible to sexual exploitation and further manipulation.[50] Subject matter experts interviewed for this research explained that perpetrators can capitalise on the nature of online gaming (which inherently involves challenge, progression, and reward), assisting vulnerable users to achieve their goals through the gifts they provide, and earning their trust.

The researchers in this study were able to purchase gift cards related to a gaming platform and distribute them by email so that recipients could redeem and apply them to their chosen account (see Box 7.1). The gaming platform had no way to track which accounts have exchanged gift cards or to detect suspicious activity around gifting.




### Box 7.1 Research insights

On **Platform N**, users can purchase gift cards through the associated website (not in-platform) and send these to 'friends' via an email address. The recipient can then redeem the gift card and apply it to their chosen account.

There is no restriction on adult users purchasing these for child users, and there is no way of **Platform N** tracking which accounts have exchanged gift cards as it is not required to input an email during user account registration.

The study identified two particularly risky features related to gifting and rewards:

1. The **ability to purchase and email electronic gift cards directly to children's personal email accounts**. This facilitates malicious actors to groom child users and has a much lower risk of being noticed when compared with the gifting of physical goods.
2. The **ability for adult users to purchase and gift paid memberships to children**, providing them with premium services. This can be used as a grooming tactic and is relatively hard for third parties to detect.

## 7.3 Proposed changes to feature

| | Potential solution | Description |
|---|---|---|
| 1 | Introduce restrictions to the purchase and giving of gift cards to users of the platform | Limit gift card transactions to registered users only, so that platforms can more accurately track how users are gifting each other. |
| 2 | Restrict adult users from gifting items or rewards to child users | Restrict the ability of adult users to purchase and transfer any form of monetised feature to a child user. This should be coupled with a robust age assurance strategy that effectively distinguishes between adult users and child users.<br><br>Child users would only be able to receive gift cards from others if they are trusted adults who have access to the child's account and can make the purchase through that account. |
| 3 | Include gifting and rewarding between accounts as a key indicator of grooming | Classify the purchase and transfer of gifts between users as a key indicator of grooming. This indicator should prompt further investigation of the nature of the contact between users, and the application of automated technologies to detect grooming language. |

### Commentary on Ofcom's Illegal Content Codes of Practice

Ofcom's Codes make almost no mention of gaming services, and do not reference the risks associated with gifting and rewards. The solutions above offer protections to children – including girls – against malicious actors who could leverage in-game gifting systems to develop trusting relationships and target them with online contact abuse.

# 8 Preventing harm to girls through child-centred design

So far, this report has focused on specific design features that enable or enhance opportunities for malicious actors to target girls with abusive communication. These risky design features, which can lead to harm either individually or in combination, should not be viewed in isolation – they are part of a broader, systemic flaw in the design of online services whereby children's safety, and the social and developmental factors that have a bearing on children's online behaviour, are largely overlooked.

Risky design features are symptomatic of the inconsistent implementation of child-centred design principles. This chapter explains how the absence of these principles results in platforms that are poorly suited to the needs of child users (who make up a third of all internet users globally);[51] and argues that child-centred design principles are necessary for mitigating online contact risks in today's platforms and in emerging technologies.

## 8.1 Design principles should be child centred

Digital platforms are designed with commercial objectives in mind. Risky design features stem from a business model whose aim is to drive up the platform's commercial and advertising revenue by extending its reach and the time users spend on it.[52]The features and functionalities identified as risky in Chapters 2 to 7 of this report are part of a broad array of tactics used by technology companies to encourage users to increase their online networks, online consumption, and online activity, often at the expense of child users' safety.[53]

Risks to girls would diminish if the design of platforms were to prioritise children's rights instead. Children should enjoy various rights in relation to the digital environment[54] – when designing digital products, children's protection from harm and their best interests are among a range of considerations that must be taken into account. There are now several frameworks in existence that set out child-centred design principles and provide guidance to developers for how to integrate children's rights into their design process.[55,56,57] Adopting a safety-by-design approach when developing digital services and products that children use would also serve to protect children's rights.[58]

To be effective, child-centred design principles need to be adopted from the outset, applied consistently throughout the design process, and implemented holistically across platforms. At present they are not, leaving major gaps in the protection of girls. This is most readily apparent when looking at the way that age assurance and default privacy settings are designed.

### 8.1.1 Poor design: age assurance

A fundamental element of child-centred design is the ability to distinguish child users from adult users. Accurate age determination is important as it can lay the groundwork for additional protective measures like age-specific filters, safety settings, and parental controls, as well as non-technological safeguards like parental supervision and discussions about online safety and wellbeing.[59]

Historically, platforms' efforts to differentiate children from adults have been underwhelming. Many rely on weak age assurance measures like self-declaration[60] that can be, and often are, bypassed by users.[61,62] This was clearly demonstrated in the present study: most of the platforms under investigation either relied solely on self-declaration or implemented no age assurance measures at all at registration. Notably, none of the 10 platforms successfully identified instances where the researchers had falsified their age by registering as a fictitious 14-year-old girl.

While platforms that are popular with children use a range of age assurance mechanisms, there is currently no clear consensus on best practice.[63] Experts suggest that a single age assurance measure is unlikely to be sufficient on its own, and that multi-faceted strategies are needed to reliably determine the age of users. Several of those who were interviewed for this research suggested that behavioural analytics, which are widely used in the financial sector, are critical in estimating identity and age and should be applied to online services used by children. Most of the platforms in this study publicly report using behavioural analytics to some degree, but details about the nature and application of these mechanisms are kept confidential.

> *"Using deepfake injection, I could fake a [facial age estimation] test. There are guides online and a determined perpetrator will always find a way. Behavioural analytics are much harder to spoof."*
>
> *Expert interview (financial sector)*

Child-centred design should also consider whether it is appropriate for young children, older children, and adults to share the same digital spaces without clear boundaries, or the application of tailored features to protect vulnerable users. In this study, only one platform offered the 14-year-old girl user the option to exist in spaces reserved solely for children. Some labelled areas on the platform as only being suitable for adults but nonetheless allowed child users to enter them. Others had no measures in place to restrict adults from interacting with the 14-year-old girl or her peers, a situation that poses significant risk for girl users.

### 8.1.2 Poor design: privacy and safety settings

The ways in which children interact with online services and with other users are shaped, in part, by their age and stage of development.[64] To create safer online environments, design must recognise childhood development and the evolving capacity of children[65,66] and provide suitable settings, experiences and interactions for children on that journey. This requires that platforms give careful consideration to how privacy and safety settings can be customised for the needs of different ages and individuals. They must also consider the defaults that are applied to users with differing levels of maturity.

The platforms in this study had mostly static, unintuitive, and over-simplified privacy and safety settings; these were not always suited to the complexity of interactions that can occur on platforms. All 10 platforms offered options to limit discoverability and interaction; but, whereas some of the platforms automatically defaulted to the most private settings for users under the age of 16,[67] safe defaults were not the norm. This is problematic because initial settings can be 'sticky', with users having a strong tendency to continue with an initial choice or with a default setting[68] even if this was not designed with users' best interests or safety in mind.

It is worth noting that default settings could be overridden in all the platforms under investigation. While some gave clear, age-appropriate explanations to help children understand the value of safer settings, this was far from universal. Without clear explanations, default settings are at risk of being misunderstood or changed, leaving children disempowered.

### 8.1.3 Poor design: social and developmental factors

The 10 platforms examined in this study have high usage rates among children: it would be reasonable to expect these services to anticipate that children would be among their users and design with their capacity and attributes in mind.[69]

This means recognising that this subset of users may be particularly eager to explore and construct their self-identity through their online profile[70], but may not have the developmental capacity to appreciate privacy risks[71] or have the baseline knowledge about online safety to decline requests to disclose personal information that is made visible to others.

It means acknowledging that child users may feel motivated to pretend to be older than they are, either to access platforms that have minimum age requirements[72] or because they do not want a limited experience on that platform, even though they understand that age assurance measures are there for their safety.[73]

It also means recognising that circumstances, social pressures, and developmental needs and vulnerabilities make this subset of users susceptible to engaging with strangers online. Circumstances like loneliness can play a part in a child's decision to interact with unknown others, but so too can developmental factors that heighten feelings of curiosity and thrill-seeking or a desire for sexual experimentation, depending on the child's age and level of maturity.[74,75] A propensity towards risk-taking for some, coupled with an under-developed appreciation that risks can apply to them, may reduce qualms about accepting connection requests from strangers.[76] The desire for social validation, often measured in terms of popularity – which, on online platforms, is made visible through numbers of likes, friends or followers – adds another layer of pressure, encouraging children to collect followers or friends indiscriminately, accept connection requests from strangers, or follow back unfamiliar profiles.[77]

*"The social validation sphere present online creates a pressure to follow back, accept a friend request, or respond to direct messages from strangers."*

*Expert interview (civil society organisation)*

Yet there are very few indications that platforms are designed with these considerations in mind. This study has provided examples of platforms that prompted a 14-year-old girl user to enter personal information that would be visible to strangers (Chapter 2); where it was possible for strangers to find her and identify her as a girl (Chapter 3); where she was encouraged to connect with others and where others were able to connect with her (Chapter 4); and where users who she may be connected to but barely know could communicate with her directly (Chapters 5 and 6). The responsibility to resist the platform's invitations to share her information and to reject approaches from strangers was placed almost entirely on the girl user.

## 8.2 Child centred design principles for the future

Emerging technologies are rapidly reshaping the digital landscape, introducing transformative capabilities while simultaneously amplifying existing risks and creating new vulnerabilities. Generative Artificial Intelligence (Generative AI) and immersive technologies are two examples of emerging technologies whose design can be exploited by malicious actors to target girls with abusive communication. ,

Generative AI holds immense potential to enhance online experiences but also poses risks to children's safety. Among these is the possibility of using generated outputs, such as fake child profiles or deepfake personas, to approach and form connections with child users for the purposes of grooming, sexually harassing, or sexually extorting them. As Generative AI outputs become more realistic and models improve and become easier to use, access, and adapt (if they are open source), sexual communication risks – which in the online world tend to disproportionately affect girls – will become more common. If models are not designed in a child-centred way, with guardrails built in from the start and embedded throughout the models' development, release, and maintenance, girls will be at even greater risk of abusive communication in the future.

Similarly, there is evidence to suggest that immersive technologies like virtual reality (VR) have increased the risk of sexual harm to children, with recent research finding evidence of sexual grooming, sexual harassment, and child sexual abuse simulations in virtual environments, alongside indications of a range of other sexual risks. Each of these risks was facilitated by the design characteristics of VR platforms. Technology companies need to take appropriate steps to embed safety-by-design in t heir products; if they do not, sexual risks can be expected to become more common as immersive technologies spread.

Looking to the future, the most assured way of tackling the risks associated with evolving technologies and new digital products is to design them from the outset with children in mind. Adopting child-centred design principles and consistently implementing these on new products will help anticipate, detect and eliminate online harms before they occur.

In the short term, more affordances could be given to users, especially to child users, so they can become accustomed to the workings of new technology. All the platforms in this study assumed that child users could operate maximum risk awareness, and that they would be prepared to protect themselves from risks immediately after registering. This is counter-intuitive, as the operation of most platforms – especially the most nascent of the 10 – takes time for users to understand. New users may find it helpful to have a protected time period after registering on products that use new technologies, during which particularly risky functionalities or interaction modes are restricted.



## 8.3 Action points for technology companies

**Consideration should be given to supplementing the potential design solutions proposed in Chapters 2 to 7 with the following actions:**

1. Publish a set of child-centred design principles and ensure these underpin the development of their products. Actively demonstrate their continued and consistent use throughout the development, release and maintenance of products.
2. Use effective age assurance technologies to reliably determine the age of users and to inform the experiences of child users at different stages of development.
3. Remove the assumption (that is currently inherent in the design of many products) that child users have the developmental capacity to appreciate risks, or the baseline knowledge about online safety to keep themselves safe.
4. Recognise the evolving capacity of children, appreciating that a young child will have different needs from an adolescent or pre-adolescent. Reflect this in the design of products and consider disabling particularly risky features and the ability to override default settings for younger children.
5. Recognise that children's online behaviours are subject to social and developmental factors that make them susceptible to engaging with strangers online. Design safety measures and default safety settings accordingly and empower child users with safety education.
6. Recognise that risk does not arise from use of a single platform but is instead a product of a user's entire digital footprint. Assess risk across platforms, particularly where there are interfaces like single sign-on or the ability to import contact lists.

Safety-by-design is arguably one of the most effective ways to protect girl users; but this should not simply translate into placing restrictions on what they can do. Protective measures need to consider and balance a range of children's rights and should not unnecessarily limit the ability of girls to express their identities or access functionalities that they may benefit from. At the same time, the right to digital participation and self-expression must not come at the expense of the right to safety. Technology companies need to weigh up how their design choices impact girl users and offer justification for retaining design features that expose them to risks.

# 9 Conclusion

Whether online or offline, girls face a disproportionately high risk of receiving abusive communication. Technology has enabled this type of abuse to infiltrate private spaces, amplifying its scale, and allowing perpetrators to act anonymously or with perceived impunity. Platforms like social media and gaming, while vital for connection and entertainment, expose girls to a range of online contact risks including sexual harassment, sexual solicitation, intimate image abuse, technology-assisted child sexual abuse, bullying, threats, extortion and hate speech.

This study sought to understand how online service design can be exploited by malicious actors to identify users who are young and female, and to target girls with harmful or abusive communication. It explored the user journey that a fictitious 14-year-old girl user would go through when registering and using 10 popular platforms and gained additional insights through a combination of desk research, interviews with subject matter experts, and practical experimentation on the 10 platforms. The abusability testing approach exposed a range of design features that can inadvertently put girl users at risk of receiving abusive communication from strangers. These design features reflect a broader, systemic flaw in the design of online services: namely, a disregard for child users' safety, their rights, and their capacities, needs, and expectations.

Twenty-seven suggestions were offered for practical changes that technology companies could make to reduce communication risks from strangers without unduly affecting the platforms' essential functionality. The proposed changes are summarised in the table overleaf.

These suggestions are offered with the explicit intention of safeguarding girls; but, if implemented alongside the recommendations for safety measures in Ofcom's Illegal Content Codes of Practice (and the more recently published Protection of Children Code of Practice) , they could make a significant difference in protecting children more generally, not just girls, from being targeted with abusive communication by other users.

As with all product development, these changes should be subjected to abusability testing before a decision is made on whether to release revised products to the public. The potential impact of their introduction on children's rights, and any potential optimisation of one right at the expense of another, should also be carefully evaluated. Moreover, the way that one design change might interact with other changes, and with other existing features, should be tested for unintended consequences, and to minimise the risk that they can be exploited to facilitate or enable harm to users. Once deployed, the efficacy of each change will need to be assessed (bearing in mind that the quality of the execution of each change also matters, and that their effectiveness will partly depend on the accuracy, robustness, reliability and fairness of the tools used to operationalise the change).

The most effective way to mitigate risk on both current and evolving digital spaces, however, is through adopting child-centred design principles; and by implementing them from the stage when a digital product is conceived and throughout its development, release and maintenance.

This research was conducted at a point immediately before the regulation of online services starts to take effect. It can, therefore, serve as a baseline record of some of the risks associated with unregulated user-to-user services. Over the coming months, we would expect platforms to carry out risk assessments to identify risky design features and introduce mitigations to safeguard their users. A repeat of this research in the future would show what actions, if any, platforms have taken to tackle the risks identified in this study, and what efforts they have made to keep girl users safe from abusive communication by strangers.

# Recommendations to improve the safety of girls online

| Online profiles | Searching for other users | Connecting with others | Direct messaging | Livestream and in-game chat | Gifting and rewards |
|---|---|---|---|---|---|
| Introduce public-facing anonymous avatars | Prevent children from appearing in the search results of adult users (unless the child's username precisely matches the 'search term' used by the adult) | Prevent adults from requesting to connect with children | Block adults from direct messaging children, unless a child has signalled that the user is trusted | Increase the lower age limit for livestreaming | Restrict the ability to purchase and give gift cards so that these can only be done on the platform |
| Automatically detect personally identifiable information in free-text bios | Prevent children from being displayed in 'recently played with' lists or 'community member' lists | Remove the functionality that allows children to import phone contacts or email contact addresses from their device | Blur or hide direct messages between users who have recently formed a connection | Prevent adults from being able to place live video calls to child users | Restrict adult users from gifting items or rewards to child users |
| Restrict the type of customisation available to young children for avatars or in-game items | Hide children's interactions with content | Provide additional descriptions of chat groups | Automatically detect and block inappropriate or offensive direct messages | Implement use of anti-screen recording technology | Include gifting and rewarding between accounts as a key indicator of grooming |
| Remove dark design patterns that encourage users to upload more information to access more of the platform | | Increase opportunities to decline and make it easier to decline connection requests | Automatically detect messages that relate to offboarding or sharing of contact details | Deploy automated language detection across environments likely to be used by children | |
| Increase the configuration of settings for presenting curated content to other users | | Implement a 'cooling off' period once connection is made between users | Integrate screenshot capability into a reporting function | Enable customisation of safety settings for each communication mode in complex multi-user environments | |
| Introduce the ability to view your own profile from another user's perspective, and remind users to do so | | | | | |

# 10 Recommendations

Based on the research findings, the NSPCC has prepared a set of recommendations for Ofcom, the UK Government, the technology sector, and researchers to consider.

## Recommendations for Ofcom

- Positively, the Illegal Harms Codes of Practice already include mitigations for some of the risky design areas identified in this report – however, significant gaps remain. Ofcom should ensure that all 27 solutions are included in the Illegal Harms Codes and, where appropriate, the Child Safety Codes. This must be a priority for the next iteration of both sets of Codes.
- This report highlights that children have evolving capacity and require different levels of support at different stages of their development. To support services to provide age-appropriate experiences for children, Ofcom should develop best practice guidance for regulated services, which outlines how safety settings and other protections can be adapted based on children's age. Ofcom should then work with service providers, especially those most popular with children, to implement this guidance.

## Recommendations for the UK Government

- Online platforms are consistently failing to effectively identify accounts belonging to under-18s and users younger than the minimum age specified in their terms of service. The Government should amend the Online Safety Act to legally empower Ofcom to require that services use highly effective age assurance to uphold their minimum age limits and deliver age-appropriate experiences.
- The upcoming Violence Against Women and Girls (VAWG) Strategy must reaffirm the Government's commitment to protecting girls online. This must include strengthening protections for particularly high-risk parts of the online world, including in private messaging and environments that facilitate complex real-time interaction between users, such as livestreaming and gaming.

## Recommendations for the technology sector

- Technology services likely to be accessed by children should commit to implementing all 27 solutions identified in this report, operationalising them effectively for their platforms.
- All services should conduct their own 'abusability studies' to identify risky features and functionalities, as well as testing any new feature before rolling it out. These tests must include a gendered analysis of likely risk.

## Recommendations for researchers

- Very few studies of online harm explore the specific experiences and risks faced by girls. To build a better understanding on online VAWG and how to tackle it, academics, civil society and Government must commit to funding and carrying out research that focuses on girls in their own right, rather than subsuming their experiences under those of the general child population or conflating the experiences of girls with those of women.
- This study demonstrated that there is value in exploring how girls use digital products. Understanding of online VAWG would benefit from more research on girls' user journeys through digital services, using either 'user experience' testing with real users, or experimentation with fake accounts, or both. Researchers should ensure that a range of identities are investigated so that intersectional experiences of harm in general – and of abusive communication in particular – can be brought to light.
- Girls face a variety of risks, both in the online world and in offline settings, and can potentially be subjected to more than one type of abusive communication. A large-scale prevalence study of child abuse in the UK is vital for getting to grips with the scale of girls' victimisation and polyvictimisation and for understanding how girls' experiences of abuse vary by their demographics and intersectional characteristics.



# References


1 NAO (2025) *Tackling violence against women and girls*. www.nao.org.uk/wp-content/uploads/2025/01/tackling-violence-against-women-and-girls.pdf

2 Plan International (2024) *State of Girls Rights in the UK*. https://plan-uk.org/state-of-girls-rights-report.pdf

3 UNFPA (2021) *Making all spaces safe. Technology facilitated Gender based Violence*. www.unfpa.org/sites/default/files/pub-pdf/UNFPA-TFGBV-Making%20All%20Spaces%20Safe.pdf

4 Girlguiding (2023) *Girls attitudes survey 2023. Girls' lives over 15 years*. www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2023.pdf

5 ONS (2024) *Bullying and online experiences among children in England and Wales: year ending March 2023*. www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/bullyingandonlineexperiencesamongchildreninenglandandwales/yearendingmarch2023#nature-of-bullying

6 Bryce, J. et al (2023) *Evidence review on online risks to children.* London: NSPCC. https://learning.nspcc.org.uk/media/ezjg0pjb/online-risks-children-evidence-review-main-report.pdf

7 Ofcom (2023) *Understanding online communications among children. Quantitative research*. www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/understanding-online-comms-among-children/quantitative-research---main/?v=330415

8 Internet Matters (2024) *"So standard it's not noteworthy". Teenage girls' experiences of harm online*. www.internetmatters.org/hub/research/teen-girls-experiences-of-harm-online/#full-report

9 Girlguiding (2024) *Girls' attitudes survey 2024. Girls face a crisis of confidence in an unequal world*. www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2024.pdf

10 Ringrose, J., Regehr, K. & Whitehead, S. (2021) Teen girls' experiences negotiating the ubiquitous dick pic: Sexual double standards and the normalization of image based sexual harassment. Sex Roles 2021 (85): pp.558–576. https://link.springer.com/article/10.1007/s11199-021-01236-3

11 Centre for Countering Digital Hate (2025) *YouTube's anorexia algorithm. How YouTube recommends eating disorder videos to young girls in the UK*. https://counterhate.com/wp-content/uploads/2025/01/YouTubes-Anorexia-Algorithm_UK_2025.pdf

12 Ofcom (2025) *A Safer Life Online for Women and Girls. Practical Guidance for Tech Companies*. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-draft-guidance-a-safer-life-online-for-women-and-girls/main-docs/annex-a-draft-guidance.pdf?v=391669

13 Ofcom (2024) *Illegal content Codes of Practice for user-to-user services*. www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-user-to-user-services.pdf?v=387711

14 Ofcom (2025) *A Safer Life Online for Women and Girls. Practical Guidance for Tech Companies*. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-draft-guidance-a-safer-life-online-for-women-and-girls/main-docs/annex-a-draft-guidance.pdf?v=391669

15 eSafety Commissioner (2024) *Technology, gendered violence and Safety by Design. An industry guide for addressing technology-facilitated gender-based violence through Safety by Design*. www.esafety.gov.au/sites/default/files/2024-09/SafetyByDesign-technology-facilitated-gender-based-violence-industry-guide.pdf

16 Wordwide Web Foundation (2021) *Tech Policy Design Lab: Online Gender-Based Violence and Abuse. Outcomes & Recommendations*. https://uploads-ssl.webflow.com/6059db55178602abe7e34c9c/60d5f88b17d5f61653d512ed_OGBV_Report_June2021.pdf

17 PUBLIC (2025) *Platform Design and the Risk of Online Violence Against Women and Girls (Online VAWG). A report for the Department for Science, Innovation & Technology*. https://assets.publishing.service.gov.uk/media/67a39e2cad556423b636cadd/Platform_design_risk_of_online_violence_against_women_girls_A.pdf

18 Daffalla, A., Bhattacharya, A., Wilder, J., Chatterjee, R., Dell, N., Tech, C., Bellini, R. & Ristenpart, T. (2025) *A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models.* USENIX Security 2025. https://pages.cs.wisc.edu/~chatterjee/papers/usenix25-passkeys.pdf

19 Brown, A., Harkin, D. & Tanczer, L. M. (2024) Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence Against Women*, 31(5), pp.1,039–1,062. https://doi.org/10.1177/10778012231222486 (Original work published 2025)

20 Ofcom (2025) *A Safer Life Online for Women and Girls. Practical Guidance for Tech Companies.* www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-draft-guidance-a-safer-life-online-for-women-and-girls/main-docs/annex-a-draft-guidance.pdf?v=391669

21 Livingstone, S. & Stoilova, M. (2021) The 4Cs: *Classifying online risk to children* (CO:RE Short Report Series on Key Topics) Leibniz-Institute for Media Research Hans-Bredow-Institut; CO:RE – Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

22 Girlguiding (2024) *Girls' attitudes survey 2024. Girls face a crisis of confidence in an unequal world.* www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2024.pdf

23 Ofcom (2024) *Consulting children on proposed safety measures against online grooming. A report based on research and engagement with children aged 13–17.* Report by Praesidio Safeguarding. www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/protecting-children/consulting-children-on-proposed-safety-measures-against-online-grooming.pdf?v=387754

24 ONS (2024) *Bullying and online experiences among children in England and Wales: year ending March 2023.* www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/bullyingandonlineexperiencesamongchildreninenglandandwales/yearendingmarch2023#nature-of-bullying

25 Revealing Reality (2023) *Without consent. Exploring image-based abuse in relationships.* www.revealingreality.co.uk/wp-content/uploads/2023/02/Without-Consent_Revealing-Reality_27Feb23.pdf

26 Storry, M. & Poppleton, S. (2022) *The impact of online abuse: hearing the victims' voice. A report by the Victim's Commissioner of England and Wales.*

27 Vulnerability Knowledge and Practice Programme (2025) *National analysis of police recorded child sexual abuse and exploitation (CSAE) crimes (2023) report for England and Wales.* https://cdn.prgloo.com/media/download/5b109756a3e-b45578a7523454c5ce0cf

28 Girls' Attitudes Survey by Girlguiding (2024) https://www.girlguiding.org.uk/globalassets/docs-and-resources/research-and-campaigns/girls-attitudes-survey-2024.pdf

29 Digital Childhoods survey by the Children's Commissioner (2022) https://assets.childrenscommissioner.gov.uk/wpuploads/2022/09/cc-digital-childhoods-a-survey-of-children-and-parents.pdf

30 UNFPA's Making All Spaces Safe report (2021) www.unfpa.org/sites/default/files/pub-pdf/UNFPA-TFGBV-Making%20All%20Spaces%20Safe.pdf

31 Ofcom (2024) *Children and parents: media use and attitudes report 2024.* www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf?v=368229

32 For comparable published examples of workflow maps, see Ofcom (2021) A-SPARC framework (Illustrative guide) and Ofcom (2023) Interactive services model

33 Centre for Countering Digital Hate (2022) *Hidden Hate: how Instagram fails to act on 9 in 10 reports of misogyny in DMs.* https://counterhate.com/wp-content/uploads/2022/04/Final-Hidden-Hate-Report-250227.pdf

34 IWF (2022) *The shocking transcripts that reveal how groomers sexually abuse children in their own rooms.* www.iwf.org.uk/news-media/iwf-in-the-news/the-shocking-transcripts-that-reveal-how-groomers-sexually-abuse-children-in-their-own-rooms/





35 Livingstone, S., Stoilova, M. & Nandagiri, R. (2019) *Children's data and privacy online: growing up in a digital age: an evidence review.* London School of Economics and Political Science, Department of Media and Communications, London, UK. https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

36 See, for example, https://saferinternet.org.uk/blog/key-things-to-remember-when-helping-your-child-set-up-a-new-profile or www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Tips-Social-media-kids-profile.pdf

37 Ofcom (2023) *Protecting people from illegal harms online. Volume 2: The causes and impacts of online harm.* Page 56. www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/volume-2-the-causes-and-impacts-of-online-harm/?v=330417

38 5Rights Foundation (2021) *Pathways: How digital design puts children at risk.* https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf

39 ONS (2023) *Children's online behaviour in England and Wales. Data from the 10- to 15-year-olds' Crime Survey for England and Wales (CSEW) on the prevalence and nature of speaking to or meeting someone online and sending or receiving sexual messages.* www.ons.gov.uk/file?uri=/peoplepopulationandcommunity/crimeandjustice/datasets/childrensonlinebehaviourinenglandandwales/yearendingmarch2023/onlinebehaviourstables.xlsx

40 Ofcom (2023) *Understanding online communications among children. Quantitative research* www.ofcom.org.uk/__data/assets/pdf_file/0027/271188/uocac-quantitative-research-main.pdf

41 Ofcom (2024) *Consulting children on proposed safety measures against online grooming. A report based on research and engagement with children aged 13–17.* Report by Praesidio Safeguarding. www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/protecting-children/consulting-children-on-proposed-safety-measures-against-online-grooming.pdf?v=387754

42 Ringrose, J., Regehr, K. & Milne, B. (2021) *Understanding and Combatting youth experiences of image based sexual harassment & abuse.* School of Sexuality Education & Association of School and College Leaders. www.ascl.org.uk/ASCL/media/ASCL/Our%20view/Campaigns/Understanding-and-combatting-youth-experiences-of-image-based-sexual-harassment-and-abuse-full-report.pdf

43 We Protect Global Alliance (2021) *Global threat assessment. Working together to end the sexual abuse of children online.* www.weprotect.org/global-threat-assessment-21/#report

44 Bentley, M. (2018) *Hopes and Streams: London Grid for Learning Trust (LGFL) DigiSafe Report on the 2018 Pupil Online Safety Survey.* www.lgfl.net/online-safety/hopesandstreams

45 Internet Watch Foundation (2018) *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse.* www.iwf.org.uk/media/23jj3nc2/distribution-of-captures-of-live-streamed-child-sexual-abuse-final.pdf

46 eSafety Commissioner (2020) *Immersive technologies – position statement.* www.esafety.gov.au/industry/tech-trends-and-challenges/immersive-tech

47 Ofcom (2024) *Children and parents: media use and attitudes report 2024 – interactive data.* www.ofcom.org.uk/media-use-and-attitudes/media-habits-children/children-and-parents-media-use-and-attitudes-report-2024-interactive-data/

48 Ofcom (2023) *Understanding online communications among children. Quantitative research.* www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/understanding-online-comms-among-children/quantitative-research---main/?v=330415

49 UNICEF (2023) *Blog post: Child Sexual Exploitation in Online Gaming. Risks and Realities.* www.unicef.org/eap/blog/child-sexual-exploitation-online-gaming

50 CEOP (no date) *Gaming: what parents and carers need to know.* www.ceopeducation.co.uk/parents/articles/gaming/

51 UNICEF Innocenti (2019) *Growing up in a Connected World. Summary report.* www.unicef-irc.org/growing-up-connected

52 5Rights Foundation (2022) '*Risky-By-Design*' https://riskybydesign.5rightsfoundation.com/introduction

53 5Rights Foundation (2021) *Pathways: How digital design puts children at risk.* https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf

54 UNCRC (2021) *General comment No. 25 (2021) on children's rights in relation to the digital environment.* www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

55 UNICEF Innocenti (2024) *Responsible Innovation in Technology for Children: Digital technology, play and child well-being.* www.unicef.org/innocenti/reports/responsible-innovation-technology-children#download

56 Montgomery, E. & Koros, E. (no date) *Meta's Best Interests of the Child Framework.* www.ttclabs.net/news/metas-best-interests-of-the-child-framework#:~:text=The%20UNCRC%20emphasizes%20that%20in,an%20important%20principle%20in%20product

57 Livingstone, S. & Pothong, K. (2023) *Child Rights by Design: Guidance for Innovators of Digital Products and Services Used by Children.* Digital Futures Commission, 5Rights Foundation. https://digitalfuturescommission.org.uk/wp-content/uploads/2023/03/CRbD_report-FINAL-Online.pdf

58 Down to Zero Alliance (2022) *Child safety by design that works against online sexual exploitation of children. Research paper from the Building Back Better programme.* www.datocms-assets.com/22233/1652864615-child-safety-by-design-report-final-1.pdf

59 eSafety Commissioner (2024) *Age assurance. Tech Trends Issues Paper.* www.esafety.gov.au/sites/default/files/2024-07/Age-Assurance-Issues-Paper-July2024_0.pdf?v=1731418892963

60 5Rights Foundation (2021) *But how do they know it is a child? Age Assurance in the Digital World.* https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

61 Ofcom (2024) *Children's online 'user ages'.* www.ofcom.org.uk/online-safety/protecting-children/online-user-ages/?language=en

62 eSafety Commissioner (2025) *Behind the screen: The reality of age assurance and social media access for young Australians. Transparency report.* www.esafety.gov.au/sites/default/files/2025-02/Behind-the-screen-transparency-report-Feb2025.pdf?v=1740397482344

63 Smirnova, S., Livingstone, S. & Stoilova, M. (2021) *Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls.* London School of Economics and Political Science (LSE). https://eprints.lse.ac.uk/112559/

64 Ofcom (2024) *Child development ages, stages and online behaviour. Overview of research and evidence.* www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/child-development-stages-review/child-development-and-online-behaviour.pdf?v=319064

65 Kidron, B. & Rudkin, A. (2023) *Digital Childhood. Addressing childhood development milestones in the digital environment.* 2ndEdition. 5Rights Foundation. https://5rightsfoundation.com/wp-content/uploads/2024/08/Digital-Childhood-Report-2023.pdf

66 Davis, K. (2023) *Technology's Child. Digital Media's role in the Ages and Stages of Growing Up.* MIT press, Cambridge, Massachusetts

67 Down to Zero Alliance (2022) *Child safety by design that works against online sexual exploitation of children. Research paper from the Building Back Better programme.* www.datocms-assets.com/22233/1652864615-child-safety-by-design-report-final-1.pdf

68 Ofcom (2024) *Behavioural insights to empower social media users. Testing tools to help users control what they see.* www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/making-sense-of-media/best-practice-design-principles/behavioural-insights-discussion-paper.pdf?v=357074

69 Kidron, B. & Rudkin, A. (2023) *Digital Childhood. Addressing childhood development milestones in the digital environment.* 2nd Edition. 5Rights Foundation. https://5rightsfoundation.com/wp-content/uploads/2024/08/Digital-Childhood-Report-2023.pdf

70 Subrahmanyam, K. & Šmahel, D. (2011) Constructing Identity Online: Identity Exploration and Self-Presentation. In: *Digital Youth. Advancing Responsible Adolescent Development.* Springer, New York, NY. https://doi.org/10.1007/978-1-4419-6278-2_4

71 Livingstone, S., Stoilova, M. & Nandagiri, R. (2019) *Children's data and privacy online: growing up in a digital age: an evidence review.* London School of Economics and Political Science, Department of Media and Communications, London, UK. www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf





72 THORN (2022) *Online Grooming: Examining risky encounters amid everyday digital socialization. Findings from 2021 qualitative and quantitative research among 9–17-year-olds.* https://info.thorn.org/hubfs/Research/2022_Online_Grooming_Report.pdf

73 Revealing Reality (2022) *Families' attitudes towards age assurance. Research commissioned by the ICO and Ofcom.* www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/keeping-children-safe-online/families-attitudes-towards-age-assurance-/drcf-ofcom-ico-age-assurance.pdf?v=328566

74 Greene-Colozzi, E.A., Winters, G.M., Blasko, B. & Jeglic, E.L. (2020) Experiences and perceptions of online sexual solicitation and grooming of minors: A retrospective report. *Journal of Child Sexual Abuse*, 29(7), pp.836–854. https://doi.org/10.1080/10538712.2020.1801938

75 Kloess, J.A., Hamilton-Giachritsis, C.E. & Beech, A.R. (2017) A descriptive account of victims' behaviour and responses in sexually exploitative interactions with offenders. *Psychology, Crime and Law*, 23(7), pp.621–632. https://doi.org/10.1080/1068316X.2017.1293052

76 Kidron, B. & Rudkin, A. (2023) *Digital Childhood. Addressing childhood development milestones in the digital environment.* 2nd Edition. 5Rights Foundation. https://5rightsfoundation.com/wp-content/uploads/2024/08/Digital-Childhood-Report-2023.pdf

77 Third, A. et al (2024) *Protecting Children from Online Grooming: Cross-cultural, qualitative and child-centred data to guide grooming prevention and response.* Save the Children International, Western Sydney University. https://resourcecentre.savethechildren.net/pdf/REPORT_PROTECTING-CHILDREN_FINAL.pdf/

78 eSafety Commissioner (2020) *Immersive technologies – position statement.* www.esafety.gov.au/sites/default/files/2020-12/Immersive%20tech%20-%20Position%20statement.pdf?v=1740408807250

79 THORN (2024) Evolving Technologies Horizon Scan. *A review of technologies carrying notable risk and opportunity in the fight against technology-facilitated child sexual exploitation.* https://info.thorn.org/hubfs/Research/Thorn_x_WPGA_EvolvingTechnologies_Dec2024.pdf

80 NSPCC (2025) *Viewing Generative AI and children's safety in the round.* London: NSPCC. https://learning.nspcc.org.uk/media/ikxlpzt2/viewing-generative-ai-childrens-safety.pdf

81 Bryce, J. et al (2023) *Evidence review on online risks to children.* London: NSPCC. https://learning.nspcc.org.uk/media/ezjg0pjb/online-risks-children-evidence-review-main-report.pdf

82 Allen, C. & McIntosh, V. (2023) *Child safeguarding and immersive technologies: an outline of the risks.* London: NSPCC. https://learning.nspcc.org.uk/media/3341/child-safeguarding-immersive-technologies.pdf

83 Livingstone, S. & Pothong, K. (2023) *Child Rights by Design: Guidance for Innovators of Digital Products and Services Used by Children.* Digital Futures Commission, 5Rights Foundation. https://digitalfuturescommission.org.uk/wp-content/uploads/2023/03/CRbD_report-FINAL-Online.pdf

84 Ofcom (2025) *Protection of Children Code of Practice for user-to-user services.* https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-protecting-children-from-harms-online/main-document/protection-of-children-code-of-practice-for-user-to-user-services-.pdf?v=395966

NSPCC

**Together, we can stop child abuse and neglect – by working with people and communities to prevent it, transforming the online world to make it safer for children, and making sure every child has a place to turn for support when they need it.**

We campaign for change. We work with schools to help children understand what abuse is and support them to speak out. Childline is here, whenever young people need us. And the NSPCC Helpline is ready to respond to adults with any worry about a child. We develop services in local communities to stop abuse before it starts and help children recover, so it doesn't shape their future.

And, above all, we work together – because everyone has a part to play in keeping children safe. Every pound you raise, every petition you sign, every minute of your time, will make a difference.

Together, we can change children's lives.

**nspcc.org.uk**

**EVERY CHILDHOOD IS WORTH FIGHTING FOR**