OCTOBER 2024

# The new face of digital abuse:

## Children's experiences of nude deepfakes

internet
matters.org

# Contents

# Foreword

**A large part of our job at Internet Matters is to stay on top of online risks, so that parents and teachers are as well-equipped as they possibly can be to keep children safe in the digital world.**

We know all too well how quickly new harms can appear and evolve in online spaces. In particular, the rapid development of generative AI (GenAI) has created previously unimagined opportunities, as well as risks, as our report on AI in education explored earlier this year.[1]

One challenge presented by GenAI is the production of 'deepfakes', which have become alarmingly common in recent years. Deepfakes – artificially generated images, videos and audio that look and feel like real content – can be used to perpetuate a number of individual and societal-level harms. This includes the spread of compelling disinformation, designed to sow mistrust in journalism, public figures and institutions, as well as the facilitation of scams and fraud.

But the overwhelming majority of deepfakes (an estimated 98%)[2] are sexual imagery, where someone's image has been imposed onto explicit content. Deepfake nudes have been in circulation online for a number of years, at least since 2017.[3] But the development of generative AI tools has marked a dramatic step-change in the ability of users to produce sexual imagery featuring real people. It is now possible to produce highly realistic deepfakes with the click of a few buttons. In the past, sexual deepfakes largely targeted female celebrities – but the accessibility of these tools means they are now used to abuse ordinary people, predominantly girls and women.

Deepfake nudes have become alarmingly common online and affect children in three ways: child-on-child sexual abuse, adult-perpetrated child sexual abuse on offender networks, and sextortion.

In recent months there have been a number of cases of male pupils creating deepfake explicit images of female classmates. Simulated nudes were shared on group chats and social media, and used to bully, extort and harass their victims. Girls describe the sheer horror and violation they felt when they discovered that they had been abused with AI-generated content, entirely without their knowledge. Tragically, deepfake image abuse has already been considered alongside the suicide of a 14-year-old girl in the UK.[4]

The Internet Watch Foundation (IWF) has also warned of a sickening surge in the volume of AI-generated child sexual abuse material (CSAM) in circulation on online offender forums. Over 3,000 pieces of AI-generated CSAM were found on a dark web forum by the IWF in just a one month period.[5]

Possession of AI-generated sexual content featuring children is illegal, but the AI models used to generate these images are not illegal – leaving them widely available to users in the UK.[6]

As a society, we have developed systems for accountability for sexual violence and harassment in the offline world. It is time to do the same in the online world and crack down on companies that produce and promote tools that are used to abuse children.

As our report sets out, children and parents are in broad agreement that more needs to be done to tackle nude deepfakes. We have used their voices and experiences to develop policy recommendations for Government and industry.

For a start, nudifying tools must be banned in this Parliament. Given the epidemic of online misogyny and violence against girls and women, highlighted by the National Police Chiefs' Council earlier this year,[7] we would also like to see the Government follow through on its commitment to strengthen the Online Safety Act in relation to gendered abuse online and AI-generated sexual imagery. In addition, there should be a greater focus on media literacy in the national curriculum, to equip children to identify deepfakes and to use AI technologies responsibly. Finally, we are calling on Ofcom to introduce stronger measures to tackle child-on-child abuse through its regulation of online platforms.

In the meantime, the tech industry should take urgent action to limit deepfake sexual abuse. Search engines should remove and de-index these services. Meanwhile, user-to-user platforms should do more to support victims to remove deepfake images after they have been shared, by investing in better reporting, content moderation and detection tools.

Alongside this report, we are also launching new resources, containing expert advice for parents on protecting children from deepfakes. However, we are clear: the responsibility must not lie with parents, children or schools to manage the fallout from this issue. We must tackle deepfake abuse at source through legislation, regulation and action from the tech industry.

As we hear from the voices of teenagers in this report, the possibility of deepfake abuse has implanted fear into children's lives. Deepfake image abuse can happen to anybody, at any time. It is time for Government and industry to take action to prevent it.

**Carolyn Bunting MBE,**
*Co-CEO, Internet Matters*
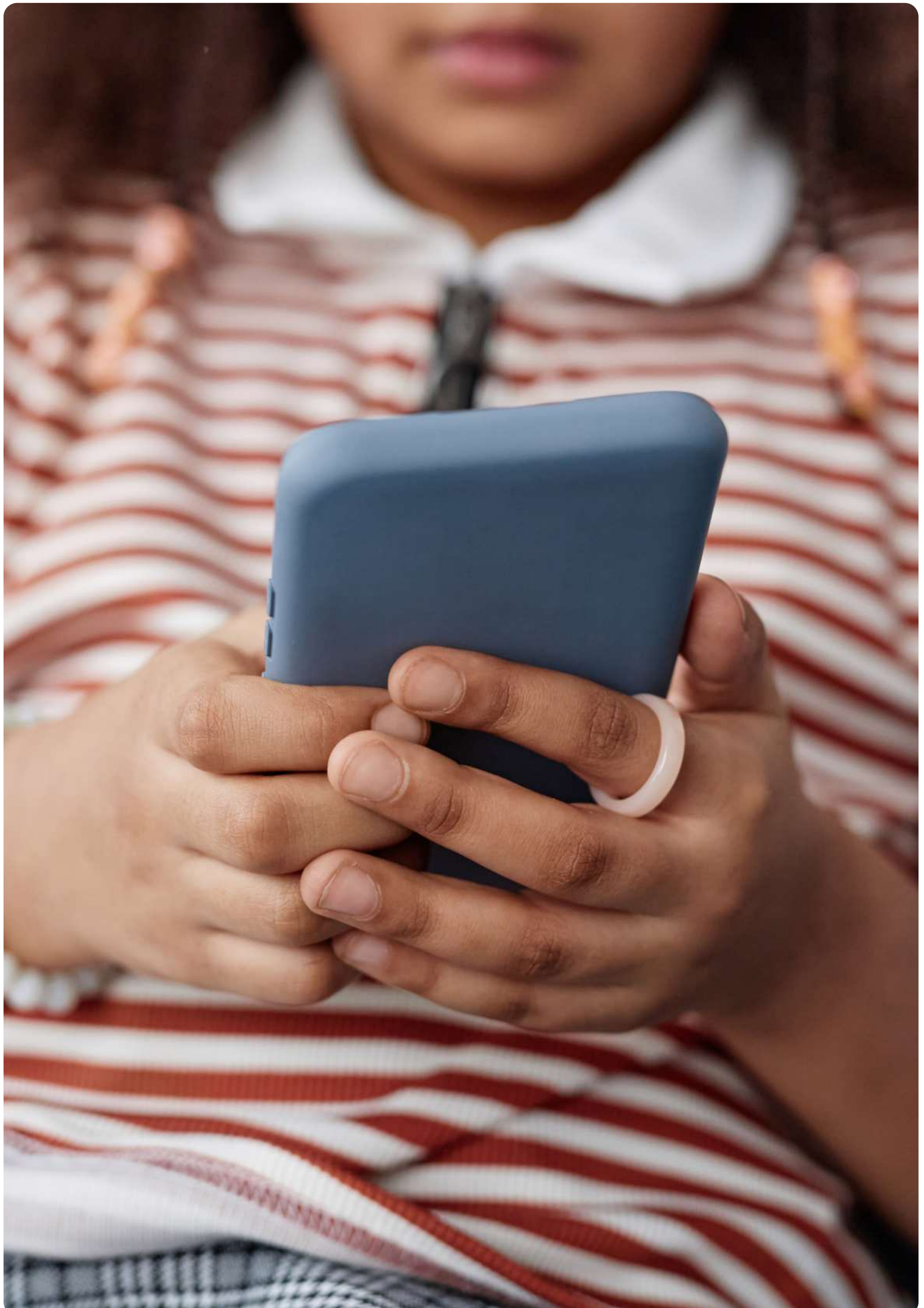
# Executive summary

This is a report exploring the issue of nude deepfakes: non-consensual sexual imagery generated with AI tools. Nude deepfakes often feature real people, including children. These images have proliferated online following the release of sophisticated generative AI (GenAI) tools. It is estimated that up to 98% of all deepfakes in circulation online are sexual, 99% of which feature girls and women.[8]

Nude deepfakes affect children in a number of ways: **child-on-child sexual abuse and harassment; adult-perpetrated child sexual abuse** including the sharing of AI-generated child sexual abuse material (CSAM) on offender forums; **and sextortion**.

This report summarises current developments in GenAI which have given rise to deepfakes and 'nudifying' tools. It also provides new evidence on families' views and experiences of deepfakes, including nude deepfakes, based on a survey conducted for Internet Matters in June 2024.

The key findings are:

## The majority of families have little to no understanding of deepfakes.

- Almost two-thirds of children (61%) and almost half of parents (45%) say that they don't know or understand the term 'deepfake'.

- Just 6% of children and 15% of parents state that they know 'a lot' about deepfakes.

The volume of deepfakes has grown rapidly online – evidence suggests that the majority of deepfakes are used for harmful purposes.

- Deepfakes aren't inherently malicious – there are positive uses of deepfakes such as education and training AI-content moderation systems. However, the evidence suggests that the majority of deepfakes are created to harm, including sexual abuse, mis- and disinformation, scams and fraud.[9]

- It is difficult to establish the true scale of deepfakes in circulation online, given that many will go undetected and unaccounted for. One study suggests that between 2022 and 2023, deepfake sexual content increased by over 400% and deepfake fraud by 3,000%.[10]

## Nudify tools are widely available online, cheap and easy to use.

- The development of GenAI has given rise to 'nudify' tools - AI models which strip the clothes from images of real people, including children. The vast majority of deepfakes online are non-consensual sexual images known as 'nude deepfakes'.

- Nudify sites and apps* are widely available online, including appearing in results of mainstream search engines. These sites advertise the ability to generate sexual imagery featuring real people within seconds, for a small fee.

- The vast majority of nude deepfakes feature girls and women (an estimated 99%). 'Nudifying' models often don't work on images of boys and men.

- AI-generated sexual imagery featuring children is illegal in the UK and is treated as child sexual abuse material under long-established child protection legislation. However, the AI models used to generate nude images of children are not illegal and are not covered by the UK's Online Safety Act.

---

*Many app providers, including Apple's App Store, have taken action to remove results for nudifying apps. However, nudifying apps have been found on the App Store as recently as September 2024 (Source).

- The sharing of nude deepfakes featuring **adults** was made a criminal offence by the UK's Online Safety Act. However, it is currently not illegal to produce consensual nude deepfakes featuring adults, as long as the image isn't shared further.[11]

## Nudifying tools are used to sexually abuse children

- Most nudify sites have terms and conditions which explicitly prohibit the production of deepfake sexual images featuring children, which is classified as illegal child sexual abuse material. However, these guardrails are often easy to circumvent – as demonstrated by the growth of nude deepfakes featuring children in both schools[12] and dark web offender forums.[13]

- AI-generated sexual images featuring children can be used to facilitate child-on-child sexual abuse, adult-perpetrated sexual abuse and sextortion.

- As with other forms of image-based abuse, deepfake nudes can impact victims profoundly, leading to the onset of anxiety, depression and suicidal thoughts.[14]

## Teenagers see nude deepfake abuse as worse than sexual abuse featuring real images.

- Teenagers are deeply concerned about nude deepfakes. The majority of teenagers (55%) believe that it would be worse to have a deepfake nude created and shared of them than a real image. Just 12% of teenagers disagree with this statement.

- The reasons for seeing nude deepfake abuse as worse than real image-based abuse include: lack of autonomy and awareness of the image, anonymity of the perpetrator, the ways in which the image may be manipulated to make the victim appear, and fears that family members, teachers or peers might believe that the image is real.

## A significant number of children have experience with a nude deepfake.

- Overall, 13% of children have had an experience with a nude deepfake, including sending or receiving one, encountering a nude deepfake online, using a nudifying app or someone they know having used a nudifying app.

- This means that around half a million (529, 632) teenagers in the UK, or 4 teenagers in a class of 30 have had an experience with a nude deepfake.

## Boys and vulnerable children are more likely to have engaged with a nude deepfake.

- Teenage boys (18%) are twice as likely as teenage girls (9%) to report an experience with a nude deepfake. For example, 10% of boys aged 13-17 have come across a nude deepfake online, compared to 2% of girls the same age. In focus groups (conducted by Internet Matters in 2023), some teenage boys told us that they had viewed nude deepfake images featuring celebrities.

- Vulnerable children are also more likely to have been impacted by nude deepfakes, compared to non-vulnerable peers. In total, a quarter (25%) of vulnerable children have experience with a nude deepfake, compared to 11% of non-vulnerable children.

- The wider literature, including previous research by Internet Matters,[15] suggests that online misogyny and pornography are shaping harmful image-sharing norms among peer groups – including the creation and sharing of nude deepfakes.

## Families are in broad consensus that Government and industry need to do more to tackle nude deepfakes.

- The majority of teenagers (84%) and parents (80%) feel that nudifying tools should be banned for everyone in the UK, including adults.

- Families also agree that more education is needed on the topic of deepfakes. Only 11% of teenagers have been taught about deepfakes in school, and just 6% about nude deepfakes in particular. The overwhelming majority of teenagers (92%) and parents (88%) feel that children should be taught about the risks of deepfakes in school. A further 92% of children and 86% of parents feel that children should be taught about nude deepfakes, in particular.

- In addition, parents are in broad agreement that firmer action should be taken by industry to tackle the issue – including preventing children from creating and encountering nude deepfakes (88%), removing nudify tools from search engine results (84%), and removing instructional advice on how to create nude deepfakes (86%). Mums are more likely than dads to support these measures.

### Legislation and industry action is needed to protect children from deepfake sexual abuse – parents and schools cannot and should not be expected to protect children alone.

- We are calling on the Government to ban nudify tools as a priority in this Parliament. The Government should also strengthen the Online Safety Act to tackle the epidemic of online violence against girls and women, by introducing a statutory code of practice on gendered harm. The Online Safety Act already mandates the online safety regulator, Ofcom, to produce non-enforceable guidance on gendered violence (Online Safety Act Section 54) – this should be strengthened to a code of practice to ensure compliance by companies in scope.

- Ofcom should introduce specific measures to tackle child-on-child abuse in its illegal harms code of practice.

- Industry should take firmer action to tackle deepfake child sexual abuse both upstream, by removing access to nudify tools from search engine results and ensuring they aren't available on app stores, and downstream by swiftly removing deepfake nude images, with priority given to images featuring children.

- The national curriculum should be updated to integrate teaching on critical media literacy, including how to spot and report a deepfake. Additionally, the Relationships and Sex Education (RSE) guidance should be updated to cover teaching about nude deepfakes, especially including the legal aspects and ethics of nude deepfakes and how to report deepfake image-abuse.

Alongside this report we are publishing new resources for parents on nude deepfakes and how to tackle this issue. Visit internetmatters.org for expert information and advice on protecting children from deepfake image-abuse.

# Introduction

**This report is a response to the growing issue of nude deepfakes, which have proliferated online with the rapid advance of generative AI (GenAI) technologies. Deepfake is a word to describe convincing AI-generated content which misrepresents the actions of someone or something.**

This report explores the ways in which GenAI has made it quick, simple and cheap to produce non-consensual explicit imagery of ordinary people – including children. Legislation has failed to keep pace with this harm – the AI models used to generate sexual imagery of children are currently not illegal in the UK, despite the fact that possession of a deepfake sexual image of a child is a criminal offence.[16]

Deepfakes can be associated with a number of harms - including mis-/disinformation and fraud – but the majority of deepfakes are sexual, which is why we have decided to focus our report on this issue.

Deepfake sexual abuse is an issue that has been affecting a growing number of children in school settings – both in the UK and around the world. But so far, little has been done to understand the voices and experiences of families – including their views on policy interventions to tackle nude deepfakes.

This report aims to address this knowledge gap. We set out to gauge the extent of awareness of deepfakes among children and parents, as well as experiences with nude deepfakes among teenagers. We also explored families' views on interventions to prevent deepfake abuse. Our aim is to inform policy development including legislation, regulation and industry action, to tackle nude deepfakes. Our findings have also informed new Internet Matters resources, containing expert advice for parents, children and young people.

Our work is based on:

- A nationally representative survey of 2,000 parents of children aged 3-17 and 1,000 children aged 9-17 in the UK, conducted by Opinium for Internet Matters in June 2024.

- Focus groups with teenagers aged 15-17 on the subjects of image based-abuse (including nude deepfakes) and online misogyny, conducted by BMG Research for Internet Matters in August 2023.

- A review of the existing literature on nude deepfakes, including grey literature.

We would like to thank the families that contributed their time to inform the findings of this report.

## Content note

**This report contains discussion of online sexual violence, including descriptions of sexual abuse. If you or a child you know is affected by the issues discussed, the following organisations can provide you with information and support.**

- **Childline** is a free service for anyone aged 18 or under living in the UK, call 0800 1111 or visit www.childline.org

- **Report Remove** is a confidential online service which helps young people under the age of 18 to remove sexual images and videos of themselves from the internet, visit www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove

- **National Crime Agency CEOP** if you have experienced online sexual abuse, or you are worried that this is happening to someone you know, you can report it confidentially to the National Crime Agency by visiting www.ceop.police.uk/Safety-Centre

- **Shout** provides 24/7 mental health support, text SHOUT to 85258 or visit www.giveusashout.org

- **Revenge Porn Helpline** is a confidential service for adults aged 18 and above experiencing intimate image abuse (otherwise known as revenge porn) visit www.revengepornhelpline.org.uk

- **Internet Matters** provides advice for parents and teachers on protecting children from a range of online harms, including nude deepfakes. Visit www.internetmatters.org

- **Take It Down** is a free service that can help you remove or stop the online sharing of nude, partially nude, or sexually explicit images or videos taken of you when you were under 18 years old. Visit https://takeitdown.ncmec.org/

- **StopNCII.org** is a free tool designed to support victims of Non-Consensual Intimate Image (NCII) abuse. It works by generating a digital 'hash' of your image, so that other instances of it can be found and taken down. Visit https://stopncii.org/?lang=en-gb
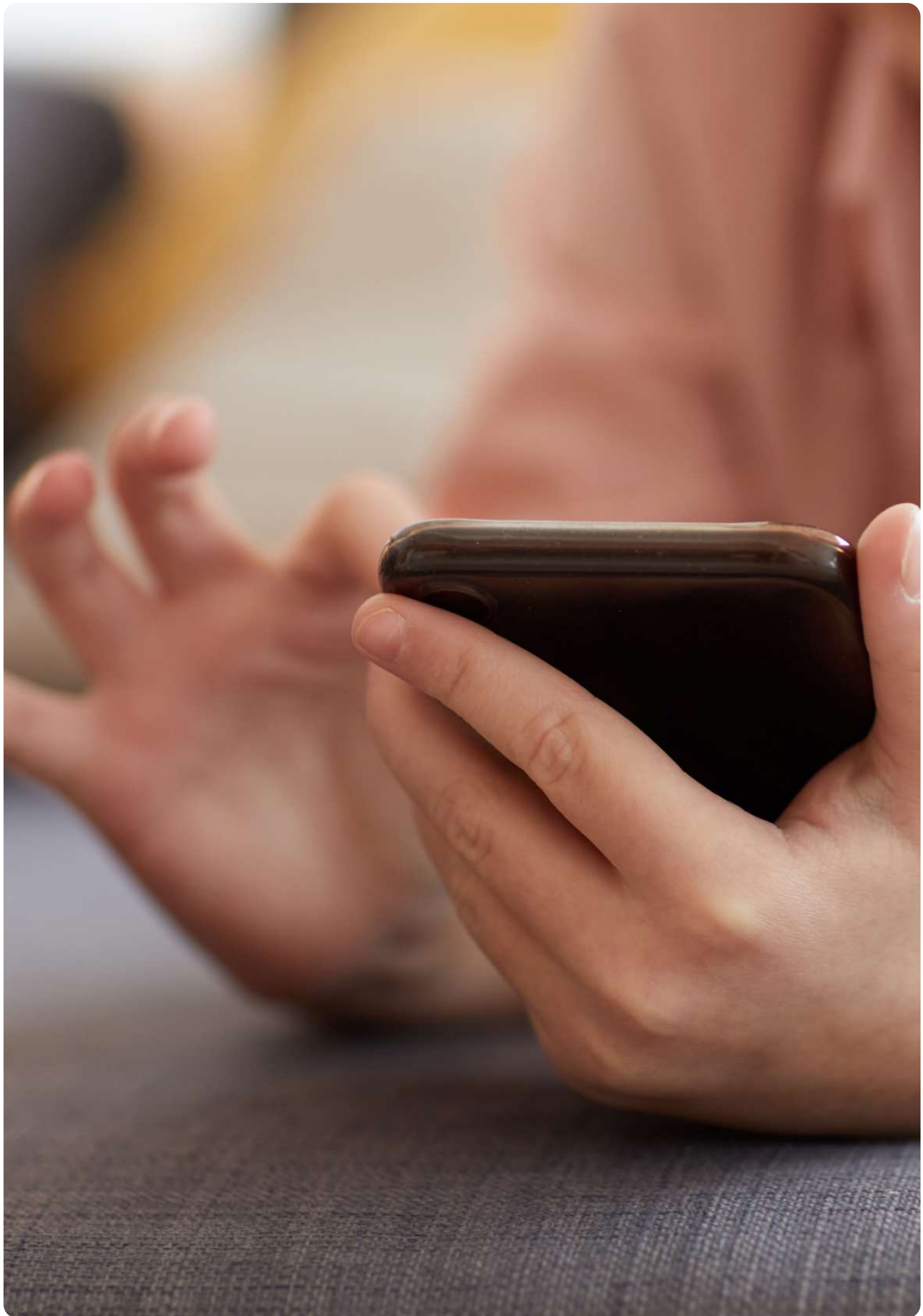
# Defining deepfakes and nude deepfakes

## What is a deepfake?

**In the simplest terms, deepfakes are fake images, videos and audio that look and feel like genuine content.**

'Deepfake' is a combination of two words, deep and fake. **Deep** refers to 'deep learning': the field of machine learning method used to generate **fake** content.

The term first emerged in 2017, when a Reddit user posted fake sexual content featuring female celebrities imposed onto the bodies of adult performers.[17] The term 'deepfake' is now used to describe a much wider set of synthetic media, although the majority of deepfakes in circulation online remain sexual in nature.[18]

In this report, we define deepfakes as **convincingly manipulated or generated audio and visual content that misrepresents the appearance, speech or actions of someone or something.** A nude deepfake is a specific type of deepfake in which **an image or video has been manipulated or generated to remove (or partially remove) clothing from someone by using their features and applying this to another body.**

In some senses, this is nothing new. Photo and video editing techniques such as Photoshop have been used for many years to manipulate visual media for use in entertainment, art and journalism. However, the rise of artificial intelligence (AI) tools has transformed the means of manipulating content and transferred the power to create deepfakes to a much wider audience of users. It now takes relatively little time or technical skill to generate a compelling deepfake.

## How are deepfakes created?

Deepfakes are created by AI tools, such as **Generative Adversarial Networks (GANs)**, **autoencoders** and **Generative AI (GenAI) models**.

GANs and autoencoders have been used for over a decade to generate realistic synthetic content. However, they require a relatively high degree of technical skill to operate. The rise of GenAI models has radically transformed the ease and cost with which deepfakes can be generated, launching deepfakes as a widespread phenomenon online.

It now takes relatively little technical skill to create deepfakes using GenAI models. With a few simple text prompts, users can create highly convincing content.

One key distinguishing feature of GenAI tools, in comparison to older technologies, is their ability to generate entirely new content. Whereas GANs and autoencoders are adept at manipulating existing content (for example adding or removing content, or swapping faces), GenAI allows for new content to be created from scratch.[19] This radically widens the possible use-cases for deepfake technology.

**Figure 1.** *An AI-generated image using text prompts on OpenAI's DALL-E. Source: OpenAI.*



DALL·E 3

A 2D animation of a folk music band composed of anthropomorphic autumn leaves, each playing traditional bluegrass instruments, amidst a rustic forest setting dappled with the soft light of a harvest moon.

## The scale and nature of deepfakes online

It is challenging to estimate the number of deepfake videos and images in circulation online, as many will go undetected. One study estimates that between 2022 and 2023, deepfake sexual content increased by over 400% and deepfake fraud by 3,000%.[20]

It is a sad truth that the overwhelming majority (an estimated 98%) of deepfake videos are non-consensual sexual imagery, of which 99% are estimated to feature women and girls.[21] Deepfake imagery is hosted on dedicated deepfake sites, as well as mainstream pornography platforms. One study estimates that there are over 275,000 deepfake sexual videos in circulation online, with 4.2 billion total views.[22] A snapshot study, conducted by the Internet Watch Foundation in September 2023, found 3,000 images of AI-generated CSAM on one dark web CSAM forum.[23]

While there are many risks associated with deepfakes, including sexual abuse, fraud and disinformation, it is important to note that deepfakes aren't inherently malicious.Artificially generated content can be used for creative and educational purposes, and deepfakes may have applications in training content moderation systems to identify harmful content at scale.[24]

## Families' awareness of deepfakes and nude deepfakes

Public concern about deepfakes was stoked in recent months following reports of pupils using AI tools to generate nude images of their female classmates.[25] Other high-profile incidents involving deepfake nude images of female celebrities,[26] as well as manipulated clips of politicians,[27] which have further heightened concern about misuse of deepfake technologies.

But while there has been much discussion in policy and tech industry circles about the applications and potential threats posed by deepfakes, little has been done to understand the views of families.

We commissioned a nationally representative survey of parents and children on the subject of deepfakes, to understand their awareness, experiences and attitudes to policy interventions.
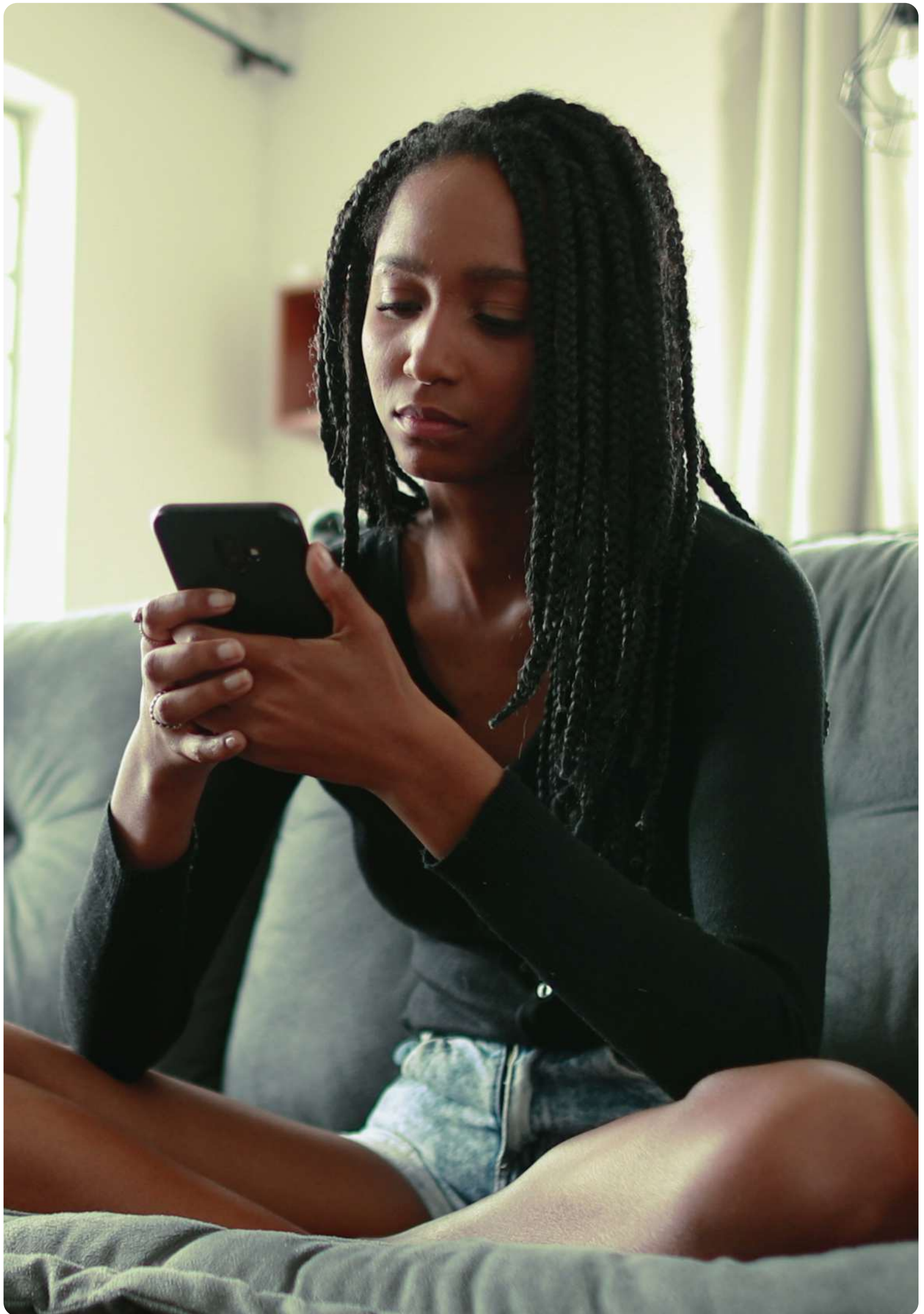
Our findings reveal that a significant proportion of both parents (45%) and children (61%) are unaware of the term deepfake.

**Figure 2.** *Percentage of children and parents who don't understand the term 'deepfake'.*
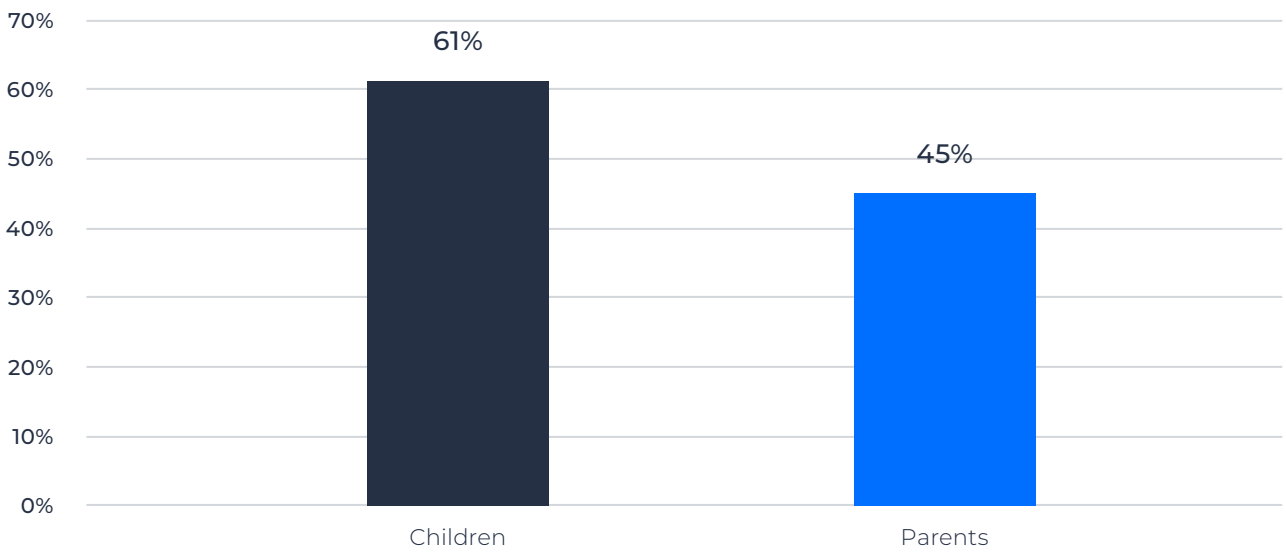


*Percentage of children aged 9-17 and parents of children aged 3-17 who don't understand the term 'deepfake', June 2024.*
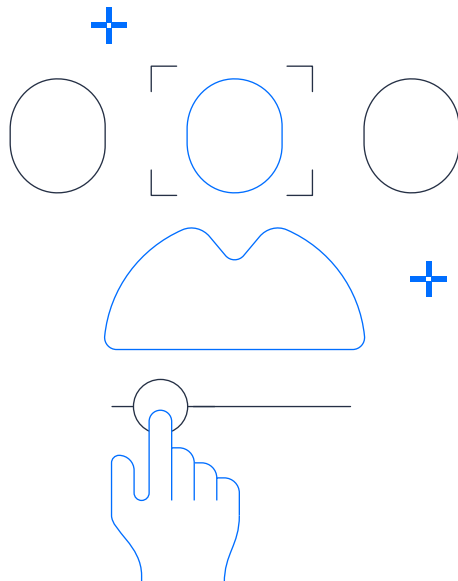
# A focus on nude deepfakes

**The remainder of this report will focus on nude deepfakes, a form of non-consensual image abuse in which clothes are artificially stripped from a subject, often real people.**

As discussed in previous sections, AI tools are rapidly developing in sophistication. It is now possible to generate highly convincing and entirely new nude images and videos with a click of a few buttons.[28]

Sexual content represents the majority of deepfakes in circulation online.[29,30] Girls and women are overwhelmingly the victims of nude deepfakes – often 'nudifying' algorithms don't work on images of boys and men.[31]

Nude deepfakes may be created for personal arousal. They are also circulated online to publicly humiliate, harass and extort victims. Nude deepfakes impact children in three main ways:

- Nude deepfakes have become a rapidly growing form of child-on-child sexual abuse and harassment in schools.[32] Teenage boys have used 'nudifying' apps to generate sexually explicit images of their female classmates, often sharing these images on group chats and social media. Discussing the topic in focus groups, girls spoke about how they would feel horrified and ashamed of the images, and would fear that a teacher or parent would think they were real, if this was to happen to them.[34]

- 'Sextortion' involving nude deepfakes has been documented. In these cases, a scammer contacts the victim with deepfake nudes (generated from social media photos) and demands payment to prevent the images from being shared further.[35] Sextortion cases involving children predominantly affect boys;[36] the impact of sextortion is devastating and has been linked to cases of child suicide.[37]

## The legality of nude deepfakes

It is important to be clear that all nude deepfakes of children are unequivocally illegal under long-established child protection laws.[39] Recent developments regarding new offences pertain to nude deepfakes of adults, rather than children. However, the tech used to create nude deepfakes is not illegal and this is where there is more work to do to protect children (and adults).

### Deepfake nude images of children

Deepfakes featuring sexual images of children (anyone below the age of 18) are illegal in the UK and classified as CSAM. Possession of any form of CSAM is a criminal offence under the Protection of Children Act 1978 and the Coroners and Justice Act 2009.[40] But the AI models used to nudify children aren't illegal.[41]

### Deepfake nude images of adults

The Online Safety Act (2023) established a new criminal offence of **sharing** a non-consensual deepfake intimate image of an **adult**.[42] The Government later announced new laws to criminalise the **creation** of a deepfake intimate image of an adult,[43] but the law did not have time to pass in the last Parliament.

The Labour Party committed to follow through and criminalise the creation of sexually explicit deepfakes of adults in its 2024 election manifesto.[44] But we are yet to see any action from the new Government and measures to tackle deepfake image abuse of adults did not feature in the 2024 King's Speech.[45]

### What this means

Nudification tools are still legal to use in the UK to create images of adults, as long as the images aren't distributed further and are consensual.

This means that nudify tools are still widely available. Some nudify sites apply safeguards to attempt to prevent users from generating CSAM. However, many AI models are open source, making safeguards easy to circumvent. The spread of AI-generated CSAM via school children and on offender networks demonstrates the fact that nudify tools are being used to sexually abuse children.

- Deepfake child sexual abuse material (CSAM) is also generated and shared by adult offenders online. The Internet Watch Foundation (IWF) found 3,000 pieces of AI-generated CSAM in a one-month period on one dark web CSAM forum.[38] Many of these images feature likenesses of real children, as well as de-aged images of adult celebrities.

## The impact on victims

Victims of deepfake sexual abuse describe the images as a profound violation.[46]

Many victims of deepfake nudes have no knowledge of their abuse. When victims are made aware of the images, it can be extremely damaging to their sense of autonomy and dignity. Many suffer PTSD, depression, anxiety and suicidal thoughts because of their experiences.[47] Victims may also fear physical violence where personal data has been shared alongside the image.[48]

Deepfake image abuse has already been considered as part of a child suicide case. 14-year-old Mia Janin tragically took her own life after being bullied by male classmates who were sharing fake explicit images.[49]

Concerningly, schools do not always treat deepfake nudes as seriously as image-abuse featuring real images.[50] This is a theme which will be explored in the next section of the report.

## What is a nudify tool?

'Nudify' tools are apps and websites that use AI models to produce deepfake nude images of real people.

In September 2024 alone, over 24 million users visited a sample of 34 nudify sites.[51] The increasing complexity and accessibility of AI models has drastically increased the number of nudify apps and sites available for users around the world.[52] For example one app, Undress.ai, processed 600,000 images of ordinary people in the first 21 days after its launch.[53]

At the time of publication, nudify tools are widely accessible in search results of mainstream search services. Searching on leading search engines for 'nudify' and 'undress' retrieves results for services that boast the ability to generate imagery of 'whoever you want' with 'accurate color, size and shape', including the ability to 'swap faces' and 'adjust expressions'. Sites urge their consumers to generate imagery 'lightning fast', 'in 3 clicks'.*

Nudify tools are available for a nominal price – with some sites offering the ability to generate an unlimited number of deepfake images for a $9.99 monthly subscription fee.

In response to a case involving AI-generated CSAM of dozens of girls in a Spanish school, some as young as 12, developers of nudifying tools brushed off any accusation of wrongdoing. The developers suggested that their tools were designed to 'make people laugh' because 'by them laughing on it we want to show people that they do not need to be ashamed of nudity, especially if it was made by neural networks'.[54] There is no age verification on these sites, meaning they are readily accessible for children to visit and use.

**Figure 3.**** *Search results for 'nudify' (retrieved August 2024)*
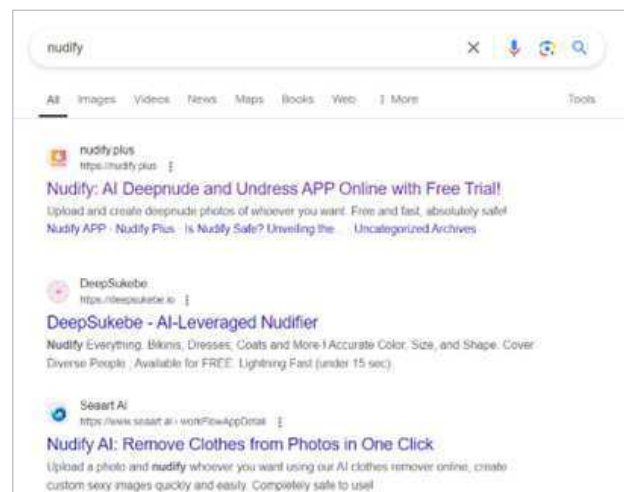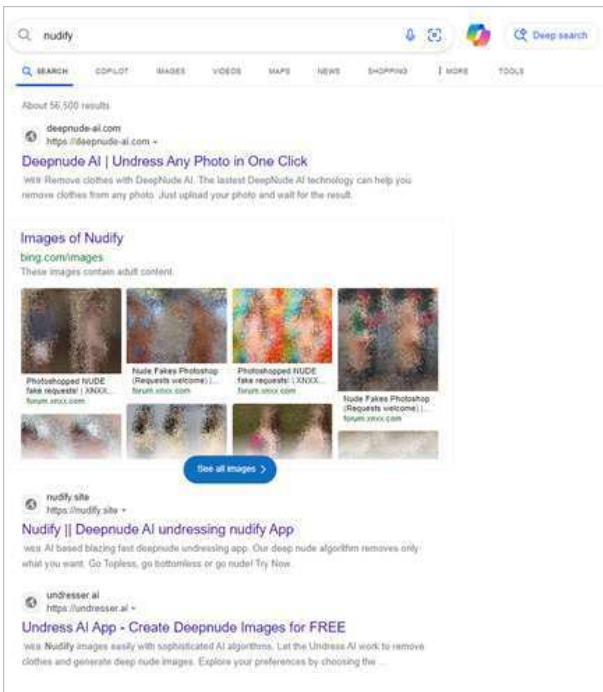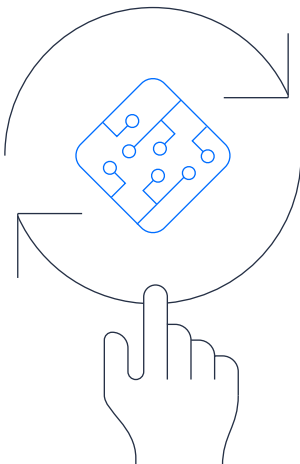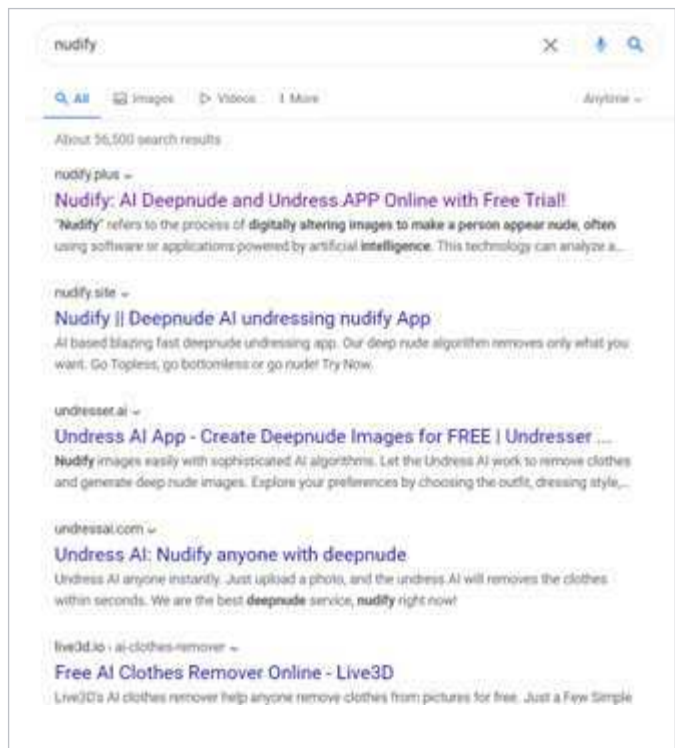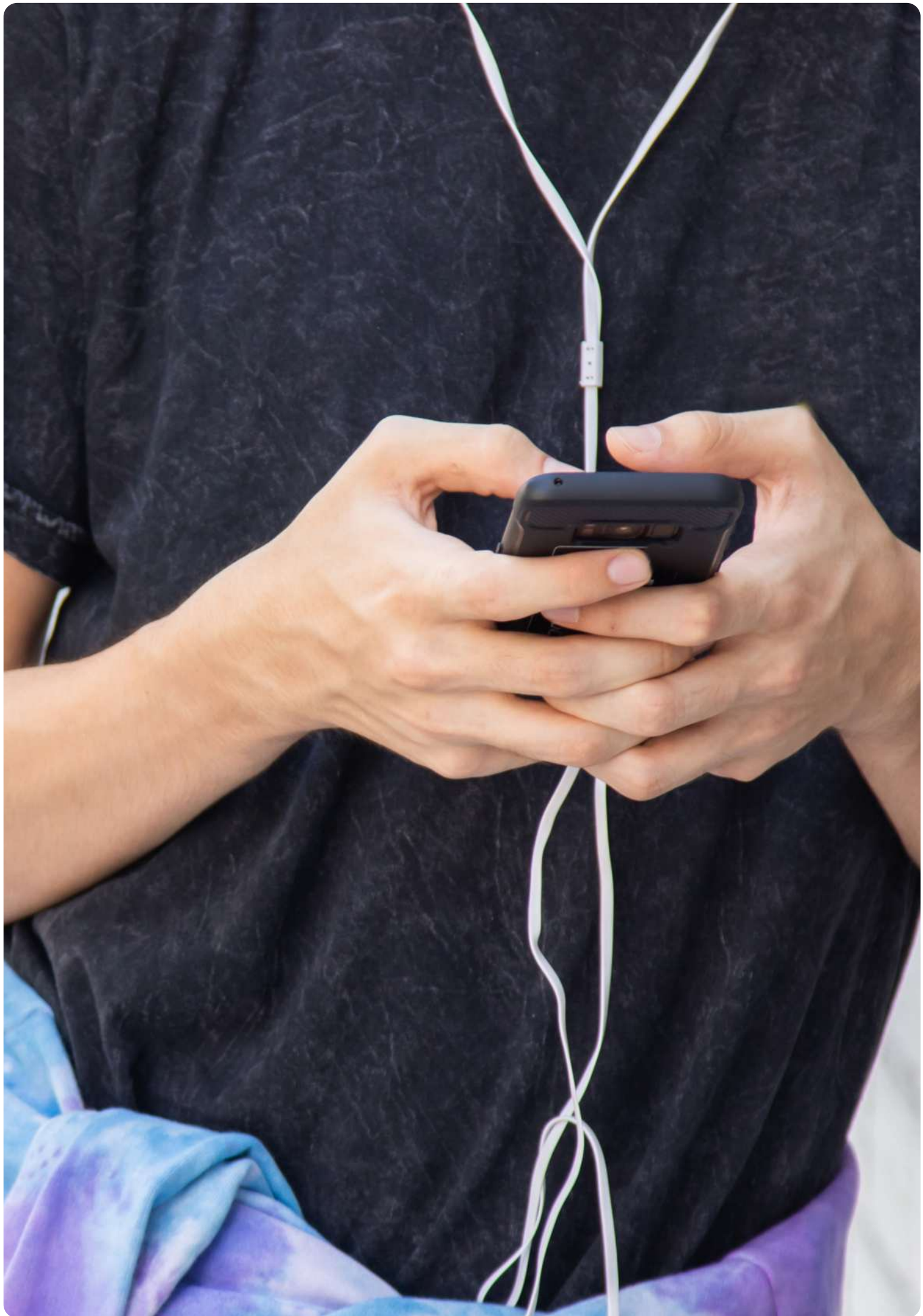


---

**Figure 4.**** *Search results for 'nudify' (retrieved August 2024)*

**Figure 5.**** *Search results for 'nudify' (retrieved August 2024)*

# Our survey: **children and parents' views on nude deepfakes**

**As with most developments in the digital space, children are already being impacted by nudification technologies – and at scale. But while there has been much coverage and discussion of adults' experiences of nude deepfakes, less research has been conducted into the views and experiences of children and their parents.**

This section sets out our research into the views of parents and teenagers towards nude deepfakes, and the extent of deepfake abuse among teenagers aged 13-17.
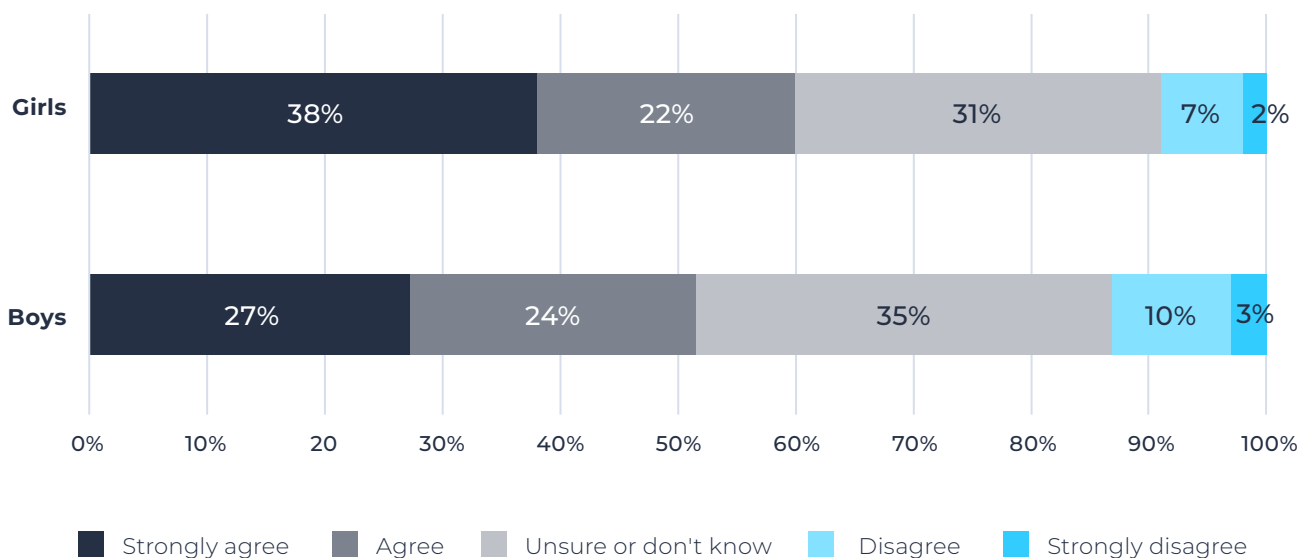
## Nude deepfakes are seen as worse than image-abuse featuring real images

Far from seeing this technology as harmless or fun, teenagers are deeply concerned about nude deepfakes. Indeed, the majority (55%) believe that it would be worse to have a deepfake nude created and shared of them than a real nude image. Just 12% of teenagers disagreed, and 33% were unsure.

Teenage girls are significantly more likely to feel this strongly – 38% of teenage girls, compared to 27% of teenage boys strongly agreed that a deepfake nude would be worse than a real nude.

**Figure 6.** *Percentage of children who agree that having a nude deepfake of them shared is worse than a real image*



Legend: Strongly agree | Agree | Unsure or don't know | Disagree | Strongly disagree

Girls: 38% | 22% | 31% | 7% | 2%
Boys: 27% | 24% | 35% | 10% | 3%

*Responses to "Having a nude deepfake of me created and shared would be worse than a real nude image of me being shared" – teenagers aged 13-17, by gender, June 2024.*

In free text responses, teenagers explained their reasons for viewing nude deepfake abuse as worse than image-abuse featuring real pictures. These findings align with previous qualitative research conducted by Internet Matters in 2023 into image-based abuse and online misogyny.[55]

Teenagers feel that deepfake nude images lack any form of consent or autonomy. In a sense, they would have a degree of involvement in the production of a real nude image – even if later sharing was non-consensual. The sense of bodily autonomy was noted in many responses, by both girls and boys:

> *"Yes. If a nude image was sent of me currently that I consented to filming even though it's sad/ unfortunate I would know that (it) was my choice that led to that image being shared. However, **with a deepfake I didn't choose for that image to be created** and its not realistic to me"* – Girl, 16, survey response

> *"I think that the deepfake would be a lot worse maybe, because, with a nude, you've taken it as well, so you know about it, whereas the deepfake, you won't have any clue at all. **There could literally be one out right now and no one could know."** – Girl, aged 15-17, focus group.*

> *"If a celebrity has taken that picture of themselves, they are aware of it. If it's just AI-generated, **they have no idea. I think that's much worse."** – Girl, aged 15-17, focus group.*

> *"I think fake ones would be a bigger impact because it'd be more of a mental struggle, because **they don't know about it, and it's not your fault."** – Boy, aged 15-17, focus group.*

Teenagers mentioned the fact that others might think the image was real, and this would have an impact on what others think of them:

> *"I would be worried **people may not realise that it was fake."** – Girl, 13, survey response.*

> *"**People would think it real** and it's not something I would do" – Boy, 17, survey response*

> *"It'd be more like, **'This is completely out of my hands.'** [...] I feel like it'd have a deeper impact, because **you know it's not you, and people think it's you**." – Boy, aged 15-17, focus group.*

Both boys and girls discussed the anonymity of the perpetrator as well as the fact that they might be unaware of the image's creation:

> *"You might never know who had betrayed you or who was trying to stir up trouble for you. **It would make me feel paranoid, like I had a stalker."** – Boy, 14, survey response*

> *"Because there is a chance **you might not know it was created."** – Girl, 15, survey response*

Teenage girls discussed concerns about the way that their body may be made to appear in a deepfake image:

> *"As the image could be **cruelly altered"** – Girl, 16, survey response*

> *"Yes, because they can manipulate worse image of me which **may seem real and damaging** than if it were real me." – Girl, 15, survey response*

Teenage girls spoke about their personal worries about being a victim of a deepfake. They describe how their fears heightened following incidents involving female celebrities and public figures:

> *"I've heard of deepfakes being used for celebrities and put up on porn sites. **That scares me** a little bit because they could use anyone's face for that. People can't tell if it's them or an AI basically, and I just find that really scary." – Girl, aged 15-17, focus group.*

*"I don't know much about it, but **I'm just scared** that they could do it for anyone really, and then they can use that."* – Girl, aged 15-17, focus group.

Boys discussed the potential harmful use-cases for a nude deepfake, such as harassment or financial sextortion:

*"It [a nude deepfake] could be used for **bullying and harassment**, in some cases."* – Boy, aged 15-17, focus group.

*"It [a nude deepfake] could be used for **blackmail**, as well. People trying to get money off people."* – Boy, aged 15-17, focus group.

Some teenage boys had encountered deepfake nude images featuring celebrities, but no participants indicated that they had created or viewed a deepfake image involving a child.

## A significant number of children have experience with a nude deepfake

Our survey suggests that a significant percentage of teenagers (13%) have had an experience with a nude deepfake. This includes teenagers who have encountered, sent or received a nude deepfake, and those who have used or know someone who has used a nudifying app.[*] This is approximately half a million (529, 632) children in the UK, meaning that 4 teenagers in a classroom of 30 are likely to have had an experience with a nude deepfake.

**Figure 7.** *Teenagers' experiences with nude deepfakes.*
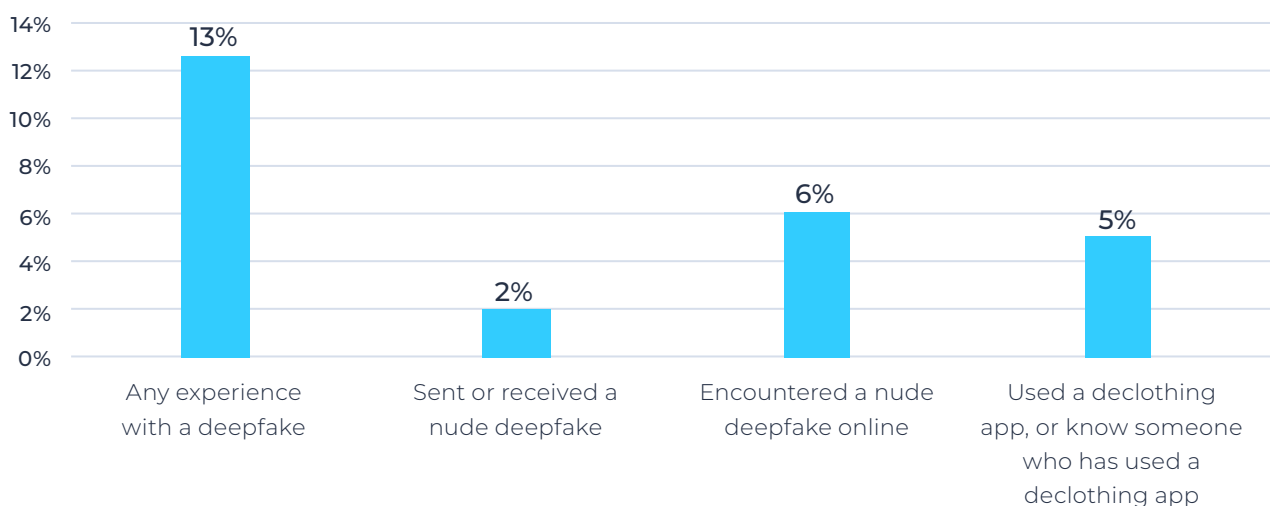


*Percentage of teenagers who have had an experience with a nude deepfake, teenagers aged 13-17, June 2024.*

*[*]Note that our survey used the term 'declothing' app to describe AI tools*

## Boys are twice as likely as girls to have engaged with a nude deepfake

We find that boys are twice as likely as girls to have interacted with a nude deepfake. In total, 18% of boys compared to 9% of girls report an experience with a nude deepfake.

In terms of specific experiences, 10% of boys aged 13-17 have come across a nude deepfake online, compared to 2% of girls the same age. 7% of teenage boys have used a declothing app, or know someone who has used a declothing app, compared to 3% of teenage girls.

## Vulnerable children are disproportionately affected by nude deepfakes

Our survey sample included a small number of vulnerable children, to understand their specific views and experiences. For the purposes of

the survey, we define vulnerability as children with special educational needs (SEN), children in receipt of an Education, Health and Care Plan (EHCP) and children with diagnosed mental and physical health conditions.

Vulnerable children are significantly more likely to experience every form of interaction with a nude deepfake assessed by our survey. Overall, a quarter (25%) of vulnerable children have had an experience with a nude deepfake, over twice the proportion of non-vulnerable peers (11%).

16% of vulnerable children have come across a nude deepfake online, compared to 5% of non-vulnerable children. 11% of vulnerable children have used a declothing app, or know someone who has used a declothing app, compared to 4% of non-vulnerable children.

These findings are supported by wider research by Internet Matters into offline and online vulnerability among young people. Our evidence consistently shows that offline vulnerabilities translate to greater risks in the online world,[56,57] including image-sharing

**Figure 8.** *Teenagers' experiences with nude deepfakes split by gender.*
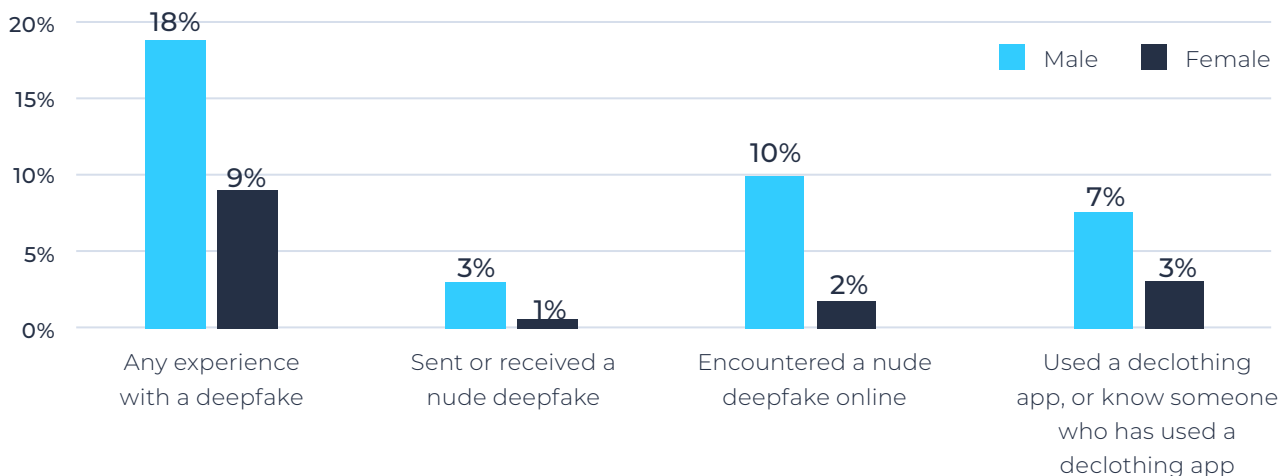


*Percentage of teenagers who have had an experience with a nude deepfake, teenagers aged 13-17, by gender, June 2024.*

and image-based abuse.[58] It appears that offline vulnerability may trigger or amplify potentially harmful encounters online, such as pressure to share personal information and intimate images, leading to higher-risk situations than peers who do not face these adversities. As we see from this research, children with offline vulnerabilities are likely to report higher rates of engagement with nude deepfakes – including being victim to a nude deepfake image,

as well as sending and receiving nude deepfakes of adults and children.

Combined with the wider evidence, this underscores the importance of tailored interventions for vulnerable young people. This should include early interventions from schools, social and health services, as well as targeted outreach to parents and caregivers of vulnerable children.

**Figure 9.** *Vulnerable & non-vulnerable teenagers' experiences with nude deepfakes.*
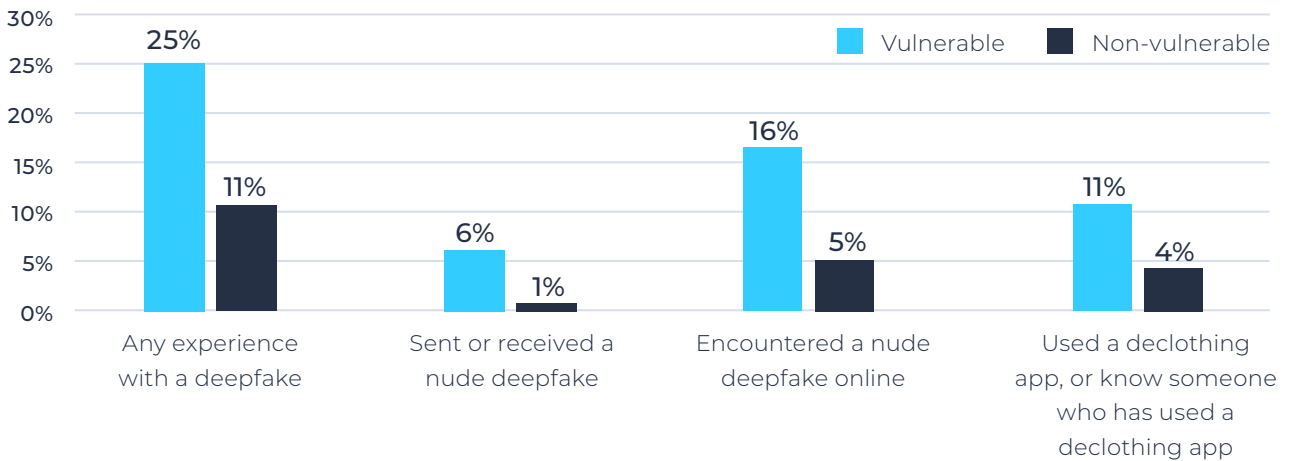
*Teenagers' reported experiences with nude deepfakes, by vulnerability, teenagers aged 13-17, June 2024.*

## The role of online misogyny in fuelling nude deepfakes

With reports of deepfake abuse in schools on the rise, we must also consider why boys are using AI technology to abuse their female classmates.

The growth in misogynistic communities – the so-called 'manosphere' – has been documented and explored in a previous Internet Matters' report.[59] Our research shows that harmful perceptions of gender, informed by online misogyny and violent

pornography, are playing a role in shaping image-sharing norms among peer groups.[60,61,62]

AI tools are offering a new avenue for boys and men to generate and commodify girls' intimate imagery. No consent, or even awareness, from the subject is needed to produce a deepfake explicit image. To be clear: not all boys and men behave this way, far from it. However, it is clear that the growth in misogynistic communities and violent pornography, coupled with technological advances, are heightening the risks that girls and women face online.
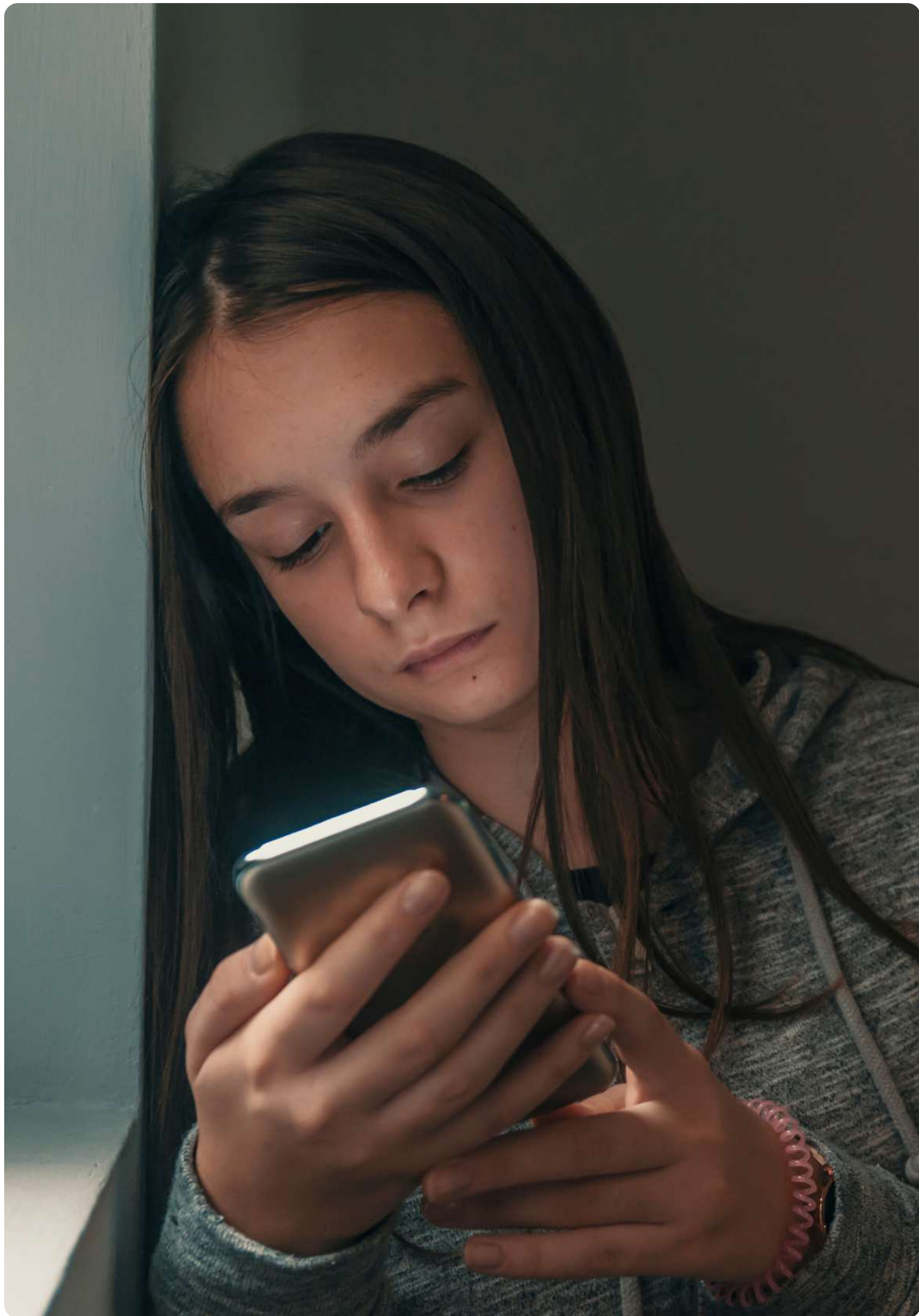
# Where next? Tackling nude deepfakes

**We are concerned that, until now, the bulk of responsibility for protecting children from deepfake image-abuse has rested with schools and parents.**

Deepfake images are not only devastating to victims, but could also result in criminal prosecution of children who perpetrate this behaviour[63] although it is important to note that policing guidelines do not always lead to the prosecution of a child in the UK**.[64]

## Families' views on policy interventions

Children and parents are in broad agreement that firmer action is needed to tackle deepfake image-abuse.

The overwhelming majority of both children (84%) and parents (80%) agree that nudifying apps and websites should be banned for everyone, including adults.

81% of children and 82% of parents feel that nudifying sites should be restricted to those aged 18 and over, as a minimum.
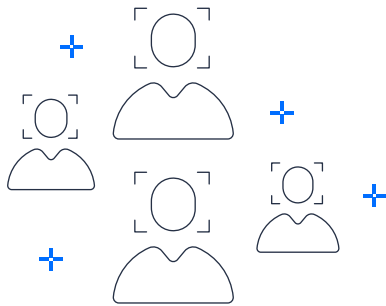
**Figure 10.** *Parents & teenagers opinions on banning declothing tools for everyone.*

*"Declothing apps and websites should be banned for everyone"*



| | Strongly agree | Agree | Unsure or don't know | Disagree | Strongly disagree |
|---|---|---|---|---|---|
| Parents | 52% | 28% | 15% | 4% | 1% |
| Children | 57% | 27% | 11% | 2% | 2% |
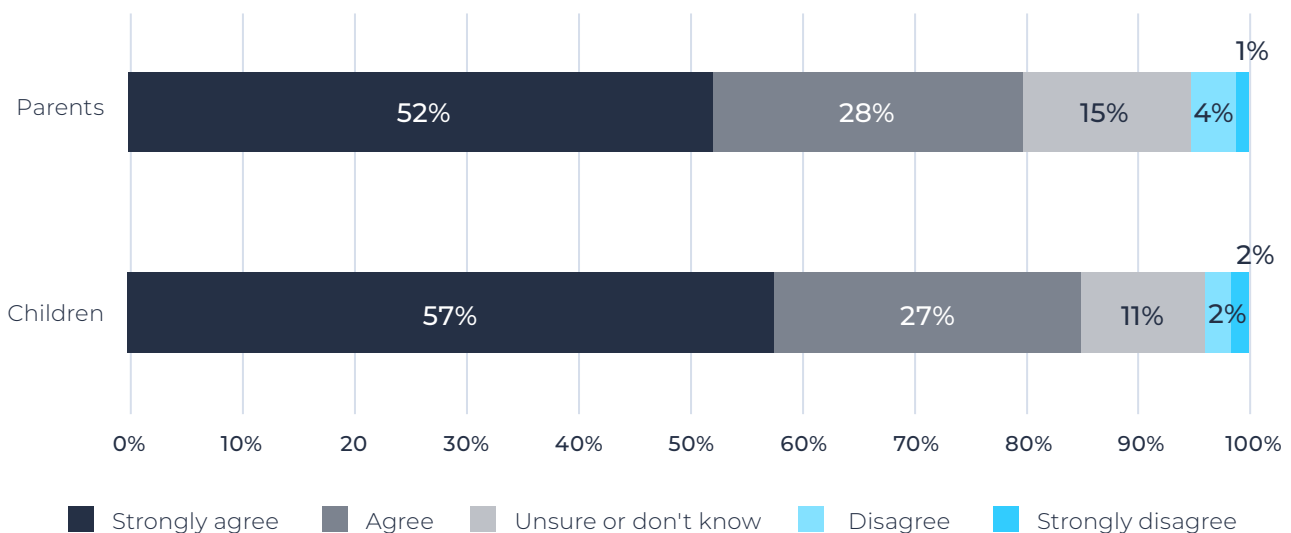
*The views of teenagers (aged 13-17) and parents (of children aged 3-17) on whether 'declothing apps and websites should be banned for everyone', June 2024.*

*\*\*Policing guidelines recognise that prosecution is typically avoided when a young person's sexting was not abusive or persistent; there is no evidence of exploitation, grooming, profit motive or malicious intent.*

**Figure 11.** *Parents & teenagers opinions on restricting declothing tools to over 18's.*

### "Declothing apps and websites should be restricted to those aged 18 and over"

| | Strongly agree | Agree | Unsure or don't know | Disagree | Strongly disagree |
|---|---|---|---|---|---|
| Parents | 56% | 26% | 13% | 3% | 3% |
| Children | 58% | 23% | 14% | 1% | 3% |
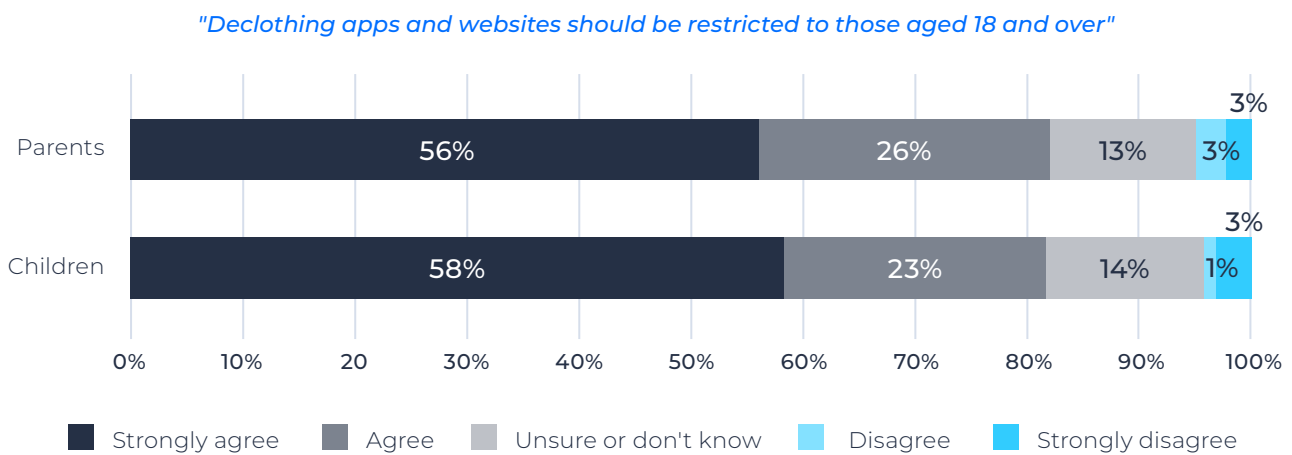
*Percentage of teenagers (aged 13-17) and parents (of children aged 3-17) who agree that 'declothing apps and websites should be restricted to those aged 18 and over', June 2024.*

We asked parents a series of further questions about policy measures to tackle nude deepfakes. The overwhelming majority of parents feel that search engines shouldn't return results for nudifying sites (84%), that instructional videos about how to create nude deepfakes should be removed by video-sharing platforms (86%) and that online services should do more to remove deepfakes and prevent children from encountering them (88%).

**Figure 12.** *Percentage of parents agreeing with each statement about deepfakes*

| More needs to be done by online services to stop children creating and / or encountering nude deepfakes (e.g., removing deepfakes from sites) | Search results shouldn't return results for de-clothing apps or websites | Information and instructional videos on how to create nude deepfakes should be removed by platforms |
|---|---|---|
| 88% | 84% | 86% |
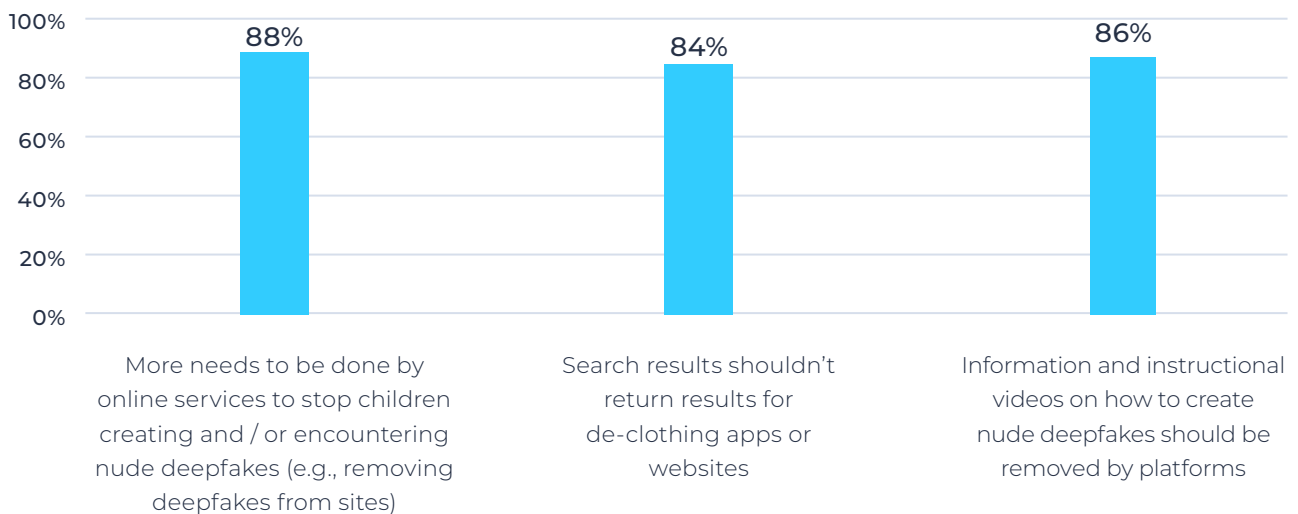
*Percentage of parents who agree with each statement about deepfakes, parents of teenagers (aged 13-17), June 2024*

Amongst parents, mums are more likely than dads to support these measures:

- More action to prevent children from creating or encountering nude deepfakes (92% of mums vs 85% of dads)

- Search results shouldn't return results for nudifying sites (87% of mums vs 82% of dads)

- Banning nudifying sites (85% of mums vs 75% of dads)

- Removing instructional advice on how to create nude deepfakes from video sharing websites (91% of mums vs 82% of dads)

## Families' views on education interventions

Our survey finds that just 11% of children aged 13-17 have been taught about deepfakes in school. A smaller percentage (6%) have been taught about nude deepfakes specifically.

**Figure 13.** *Percentage of children taught about deepfakes and nude deepfakes in school.*
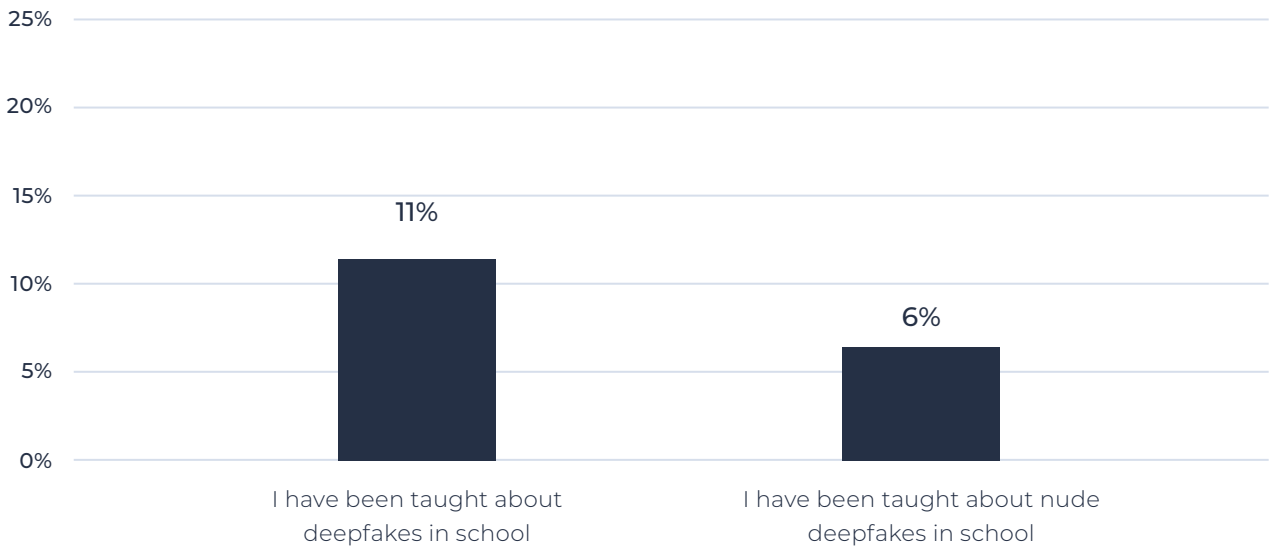


*Percentage of children who have been taught about deepfakes and nude deepfakes in school, teenagers (aged 13-17), June 2024.*

The rapid proliferation of deepfakes online, coupled with poor awareness levels among children (39% aware) and parents (55% aware), heightens the risk for families of misidentifying harmful deepfakes. Indeed, the majority of both children (72%) and parents (68%) are unconfident or unsure if they would be able to identify a deepfake. Both children and parents agree that schools should teach about deepfakes, including nude deepfakes specifically.

We find that a slightly higher percentage of children feel that children should be taught about the risks of deepfakes (92%) and nude deepfakes in particular (92%), than parents – 88% and 86% respectively.

**Figure 14**. *Percentage of children and parents who agree children should be taught about the risks of deepfakes*
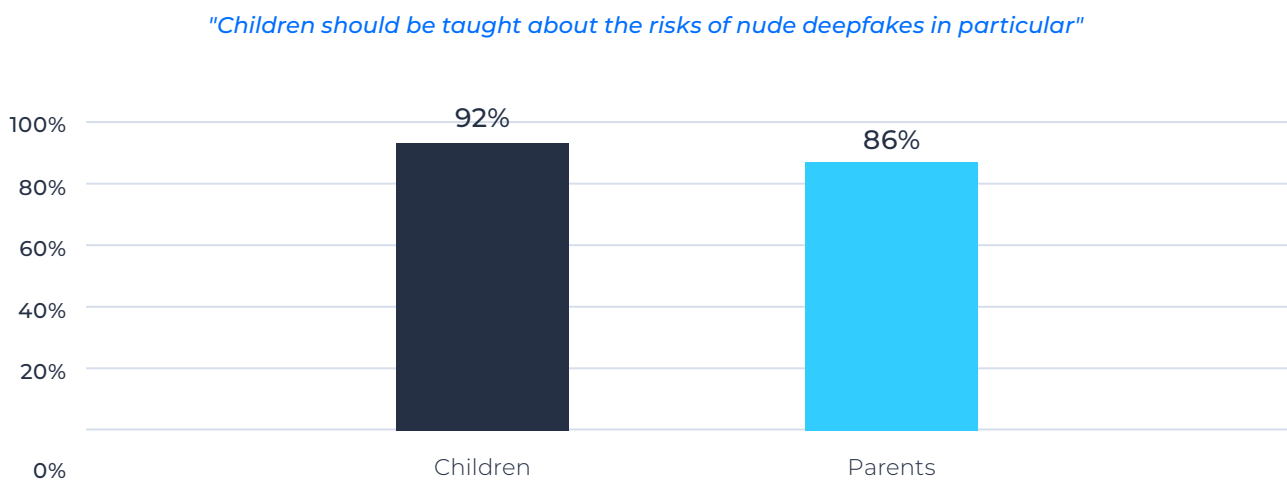
*"Children should be taught about the risks of deepfakes in general"*
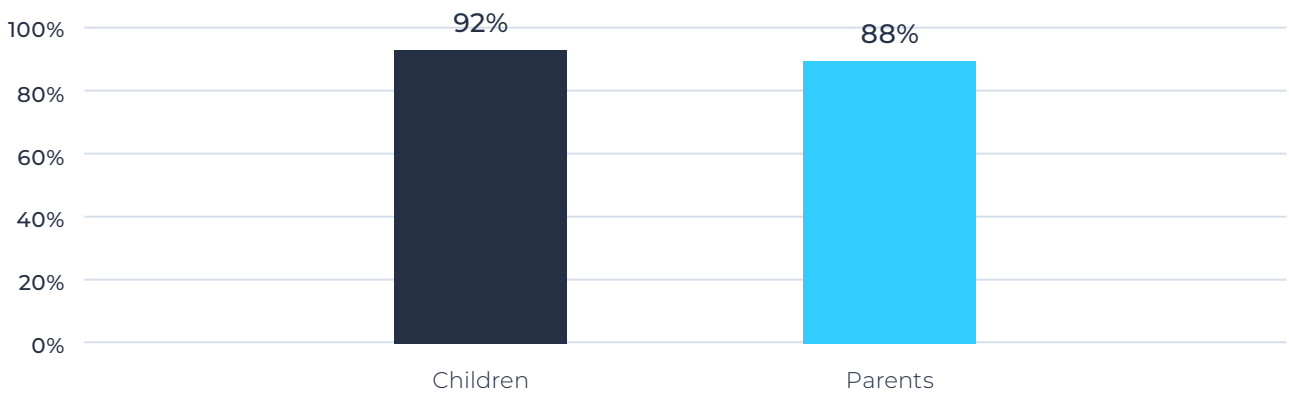


*Percentage of children (aged 13-17) and parents (of children aged 3-17) who agree that 'children should be taught about the risks of deepfakes', June 2024.*

**Figure 15.** *Percentage of children and parents who agree children should be specifically taught about the risks of nude deepfakes*

*"Children should be taught about the risks of nude deepfakes in particular"*



*Percentage of children (aged 13-17) and parents (of children aged 3-17) who agree that 'children should be taught about the risks of nude deepfakes in particular', June 2024.*

The Department for Education recently announced a full review of the national curriculum in England.[65] Following violent riots in August 2024, fuelled – at least in part – by misinformation on social media, it has been suggested that critical media literacy will be embedded within the national curriculum to equip children to identify false and harmful information.[66] As will be discussed in the conclusions and recommendations section of this report, it is important for any review of the curriculum to include teaching about identifying harmful deepfakes, and the legal and moral implications of nude deepfakes in particular, via Relationships and Sex Education (RSE).
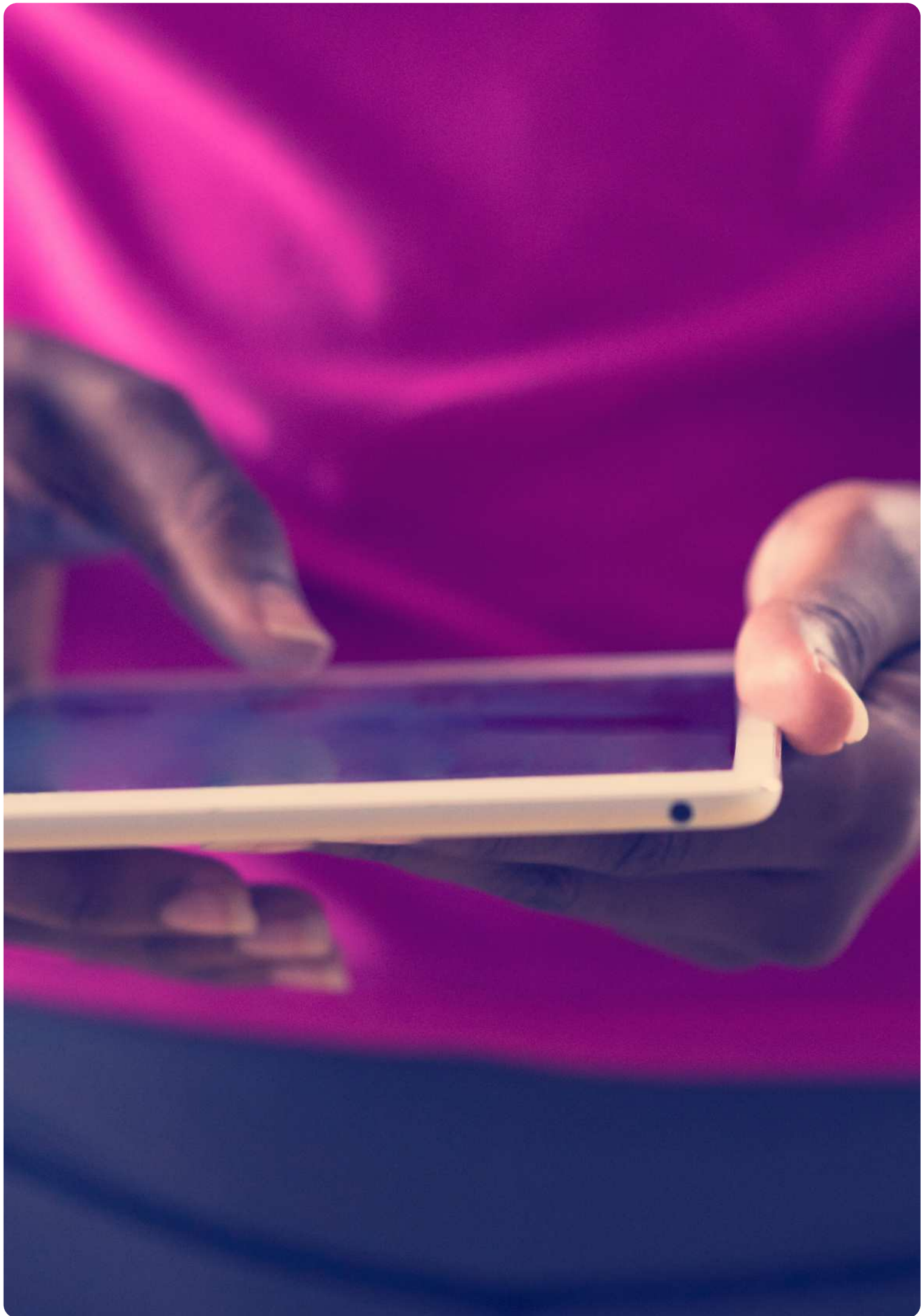
# Conclusions and recommendations

**Urgent action is needed to protect children from deepfake abuse. Nude deepfakes are a profound invasion of bodily autonomy and dignity and their impact can be life-shattering.[67] Experiencing this as an adult is bad enough, let alone as a child.**

As discussed in this report, children see nude deepfake abuse as a potentially greater violation than image abuse featuring real pictures, because it is completely out of their control.[68]

There are three primary risks to children stemming from sexual deepfakes – adult-perpetrated sexual abuse including the dissemination of AI-generated CSAM on offender forums, sextortion and child-on-child sexual abuse.

Parents and schools are currently managing the fallout from nudifying tools – but there should be firm action from various parties, including the Government, Ofcom and industry, to tackle this issue. As a priority, the Government should ban nudifying tools.

There are ongoing campaigns to criminalise non-consensual deepfake sexual imagery featuring adults – a pledge made by the last Government and in the 2024 Labour Party manifesto.[69,70] While we support the call to criminalise all forms of non-consensual deepfakes, including images of adults, AI-generated sexual images featuring children are already illegal under long-established child protection laws.[71] For this reason, a distinct approach is needed to ensure that children are kept safe from the risks of nude deepfakes.

Below are our key recommendations for Government, Ofcom and industry to address deepfake image-abuse. We also outline the resources Internet Matters has created for parents, children and young people to help protect them from the risks associated with deepfakes. We are clear that the responsibility should not rest with parents alone to protect children from nude deepfakes. But while we wait for the Government, the regulator and industry to act, it is important that parents and schools are fully informed of the risks and means to protect children from deepfakes.

## Legislation

Legislation is currently failing to protect children from deepfake image abuse. Nudifying tools are widely available and used to sexually abuse children. This is inexcusable. The Government must take urgent action in this Parliament to protect children:

- **Ban nudifying tools.** The AI models used to create CSAM are currently not illegal in the UK – this is despite strong appetite among children and parents to ban all nudifying apps and websites. The Government should act to criminalise non-consensual deepfake tools, with appropriate sanctions for developers who publish these models.

- **The Online Safety Act should be updated to cover harms from deepfake abuse within the Government's wider package of measures to regulate AI-specific risks.** The UK Government recently signed an international treaty to protect users from the potential harms of AI tools.[72] Implementation of the framework should include strengthened measures to prevent deepfake abuse including regulatory oversight of AI models before they go to market.[73]

- **Strengthen the Online Safety Act to include a statutory Code of Practice on gendered violence.** Earlier iterations of Online Safety Act were widely criticised for failing to include references to gendered violence.[74] The previous Government conceded by introducing Ofcom Guidance on protecting women and girls into the Online Safety Act,[75] but this does not go far enough. A statutory Code of Practice on gendered violence would provide stronger protections for women and girls against misogynistic and sexual violence online, including nude deepfakes.

## Regulation

By far the most important action in this space is the banning of nudification tools by Government. But there are also actions that Ofcom can take through its ongoing regulation of services to bolster children's protection from nude deepfakes. To tackle children's engagement with nude deepfakes, Ofcom should:

- **Amend the draft Illegal Harms Code of Practice to include measures to tackle child-on-child sexual abuse, including nude deepfakes.** We were disappointed that child-on-child abuse did not feature in the draft Illegal Harms Code, with only two passing references in the causes and impacts of illegal harms document.[76,77] Child-on-child abuse is a significant and growing proportion of online child sexual abuse (CSA), with 52% of reported CSA offenses now carried out by someone under 18,[78] and our own research showing the majority of image-based abuse is perpetrated by young people.[79] A differentiated approach is important because the dynamics underpinning child-on-child abuse differ from adult offending, as do the measures to combat it.

## Industry

Tech companies must take accountability for deepfake image abuse facilitated by their platforms. Services should address non-consensual deepfakes **upstream** by removing access to nudifying tools, as well as downstream by swiftly removing deepfake nudes from their platforms and taking enforcement action against offenders. While more is being done by industry to tackle the issue **downstream**, far firmer action is needed to limit access to nudifying tools to prevent production in the first place.

Specifically, we would like to see the following actions from industry:

- **Remove results for nudifying and declothing tools**. It is inexcusable that search engines are making tools that facilitate CSAM production freely available. The fastest way to prevent deepfake abuse and protect children from suffering and participating in sexual abuse is to remove search results for nudifying tools, including from app stores.

- **Offer redress to victims of deepfake abuse** by offering clear and reliable routes to report and remove search results containing deepfake nudes, and prioritising children's reports for human review. Reports of AI-generated sexual abuse of children should be referred to NCMEC in the USA or the NCA in the UK (depending on jurisdiction of the platform). Some search engines have recently announced policies to curb the spread of non-consensual deepfakes, by making it easier for victims to request that deepfake imagery be removed.[83] This is an important step, but it is secondary to removing access to AI tools that facilitate abuse in the first place.

- **Ensure that parental filters block results for nudifying tools.** Our research suggests that some parental filtering tools may fail to block access to nudifying sites. All ISPs should review and update their parental controls to ensure that children do not have access to these sites.

- **Provide reporting routes for parents and teachers as non-registered users,** as parents are the first port of call for most children when something goes wrong online.[84] Parents and teachers should have an accessible independent reporting route, which does not require sign-up to the relevant platform.

## Education

Media literacy skills among children and parents remain stubbornly poor. This means that children are interacting with harmful deepfakes at scale and parents are generally under-equipped to support their children to manage these risks. Internet Matters recently published a review of media literacy education in schools, setting out a blueprint for integrating media literacy in the curriculum.[86] From this research, we recommend that the Department for Education (DfE) should:

- **Address critical media literacy as a core component of all key stages of teaching, as part of the Curriculum Review.** The DfE should publish a media literacy framework, setting out how schools should teach media literacy through core subjects.

- **Update the Relationships and Sex Education (RSE) guidance to include teaching about nude deepfakes,** covering the ethical and legal aspects of nude deepfakes and how to report them – alongside teaching about other forms of image-based abuse. Our research shows that education about image-sharing should be delivered by expert teachers, and begin from the first years of secondary school, continuing in an age-appropriate way throughout secondary school.[87]

## Parents and young people

Parents play a crucial role in helping children stay safe online, especially in an age where regulation and legislation lags behind rapidly evolving technology. In response to our research, Internet Matters has developed resources to support parents to protect children from the risks associated with deepfakes.

- **Our parent resource highlights different types of deepfakes,** the risks associated with them and provides guidance on how to support children if they have been affected by one.

We have also developed resources for young people which aim to build resilience, enhance critical thinking, and provide support for children facing the challenges that come with deepfakes.

- **Our resources for young people outline the different types of deepfakes,** provide practical tips on how to spot them, highlight what steps can be taken to protect themselves from potential harm and provide guidance on who they can turn to if impacted by a deepfake.

# Methodology

This report was developed with a combination of quantitative, qualitative and desk research.

## Quantitative research

This report contains findings from a nationally representative survey of children and parents in the UK, conducted by Opinium for Internet Matters in June 2024.

The survey sought the views of:

- 2,000 parents of children aged 3-17

- 1,000 children aged 9-17, with some questions restricted to children aged 13 and above.

The survey contains a subsection of children (and parents of children) with vulnerabilities. For the purposes of the survey, we define vulnerability as:

- A diagnosed mental or physical health condition

- An Education, Health and Care Plan (EHCP)

- Special Educational Needs (SEN)

More information about our digital tracking data can be found on the Internet Matters' website.

Note that percentages in the graphs of this report may not all sum precisely to 100% due to rounding.

## Qualitative research

The report contains findings from focus groups with teenagers aged 15-17, conducted in August 2023 by BMG Research for Internet Matters.

## Desk research

The report is also informed by a review of the literature on nude deepfakes, including grey literature.
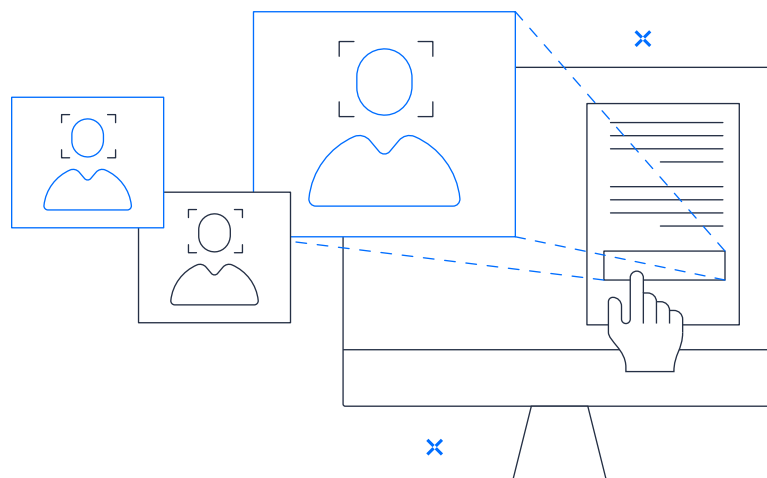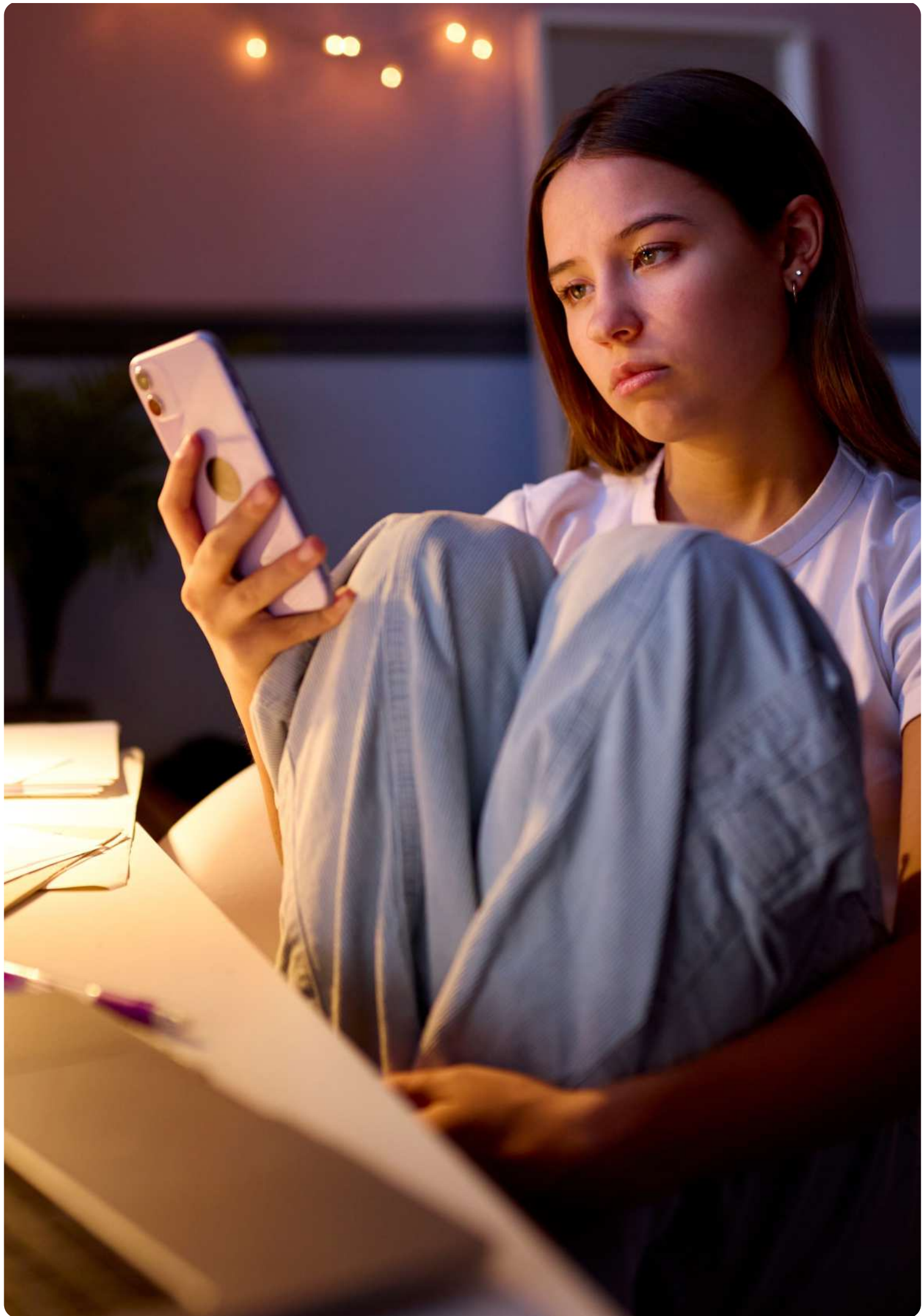
# References

1. Internet Matters (2024) Generative AI in education: Research into children's and parents' views of artificial intelligence, link.

2. Security Hero (2023) State of Deepfakes: Realities, Threats and Impact, link.

3. Somers, M. (2020) 'Deepfakes, explained', MIT Sloan School, link.

4. Metro (2024) 'Girl killed herself when bullies shared fake nudes of her', link.

5. Internet Watch Foundation (2023) How AI is being abused to create child sexual abuse imagery, link

6. Internet Watch Foundation (2023) How AI is being abused to create child sexual abuse imagery, link

7. National Police Chiefs' Council (2024) 'Call to action as VAWG epidemic deepens', link.

8. Security Hero (2023) State of Deepfakes: Realities, Threats and Impact, link.

9. Ofcom (2024) Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes, link.

10. Control AI (2024) Deepfakes: A call to action, link.

11. The Mirror (2024) 'Vile AI 'nudifying' app allowing kids to create indecent images of their classmates', link.

12. BBC News (2023) 'Children making AI-generated child abuse images, says charity', link.

13. Internet Watch Foundation (2023) How AI is being abused to create child sexual abuse imagery, link

14. McGlynn, C., Johnson, K., Rackley, E., Gavey, N., Flynn, A., Powell, A. (2020) ' 'It's torture for the soul': The Harms of Image-based Sexual Abuse, Social & Legal Studies 30(4), link.

15. Internet Matters (2023) 'It's really easy to go down that path': Young people's experiences of online misogyny and image-based abuse, link.

16. Protection of Children Act 1978 and Coroners and Justice Act 2009, see CPS guidelines (link).

17. Westerlund, M. (2019) The emergence of deepfake technology: A review. Technology innovation management review, 9(11).

18. Security Hero (2023) State of Deepfakes: Realities, Threats and Impact, link.

19. Ofcom (2024) Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes, link.

20. Control AI (2024) Deepfakes: A call to action, link.

21. Ibid.

22. My Image, My Choice (2024) Deepfake Abuse Landscape Analysis: The exponential rise of deepfake abuse in 2023-2024, link.

23. Internet Watch Foundation (2023) How AI is being abused to create child sexual abuse imagery, link.

24. Krishna, S., Johansson, P., Bright, J. (2024), 'Can synthetic data help to keep people safe online? Artificially created images, text and videos can be used to teach AI systems to recognise harmful content.' The Alan Turing Institute, link.

25. BBC News (2023) 'AI-generated naked child images shock Spanish town of Almendralejo', link.

26. BBC News (2024) 'Taylor Swift deepfakes spark calls in Congress for new legislation', link.

27. Cabinet Office (2024) Guidance: Online disinformation and AI threat guidance for electoral candidates and officials, link.

28. Jones, C. (2024) Preventing AI Sexual Abuse by Suppressing Nudification Tools, link.

29. Security Hero (2023) State of Deepfakes: Realities, Threats and Impact, link.

30. Ofcom (2024) Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes, link.

31. Law Commission (2021) Intimate Image Abuse: A consultation paper, 2.47, link.

32. Politico (2024) AI is shockingly good at making fake nudes — and causing havoc in schools, link.

33. The Times (2024) 'Private schoolboys made indecent images of female pupils with AI', link.

34. New York Times (2024) 'The Online Degradation of Women and Girls That We Meet With a Shrug', link.

35. The Verge (2024) 'Blackmailers are using deepfaked nudes to bully and extort victims, warns FBI: The agency says it's seen an 'uptick' in incidents where malicious actors use pictures and videos from social media and edit them using AI to create blackmail material.', link.

36. Internet Watch Foundation (2023) 'Hotline reports 'shocking' rise in the sextortion of boys', link.

37. Europol (2017) Online sexual coercion and extortion as a form of crime affecting children, link.

38. Internet Watch Foundation (2023) How AI is being abused to create child sexual abuse imagery, link

39. Protection of Children Act 1978 and Coroners and Justice Act 2009, see CPS guidelines (link).

40. Criminal Prosecution Service (updated May 2024) 'Indecent and Prohibited Images of Children', link.

41. Internet Watch Foundation (2024) What has changed in the AI CSAM landscape? AI CSAM report update, link.

42. Ministry of Justice (2022) 'New laws to better protect victims from abuse of intimate images', link.

43. Ministry of Justice (2024) 'Government cracks down on 'deepfakes' creation', link.

44. Labour Party (2024) Change: Labour Party Manifesto 2024, link.

45. Prime Minister's Office (2024) The King's Speech 2024: Background briefing, link.

46. The Guardian (2024) 'I felt numb – not sure what to do. How did deepfake images of me end up on a porn site?' link.

47. The Conversation (2024) 'Deepfake porn: why we need to make it a crime to create it, not just share it', link.

48. End Cyber Abuse, 'Image-based Sexual Abuse: An Introduction', link, accessed 15.08.2024.

49. Metro (2024) 'Girl killed herself when bullies shared fake nudes of her', link.

50. The New York Times (2024) 'The Online Degradation of Women and Girls That We Meet With a Shrug', link.

51. Graphika (2023) 'A revealing picture: AI-Generated 'Undressing' Images Move from Niche Pornography Discussion Forums to a Scaled and Monetized Online Business', link.

52. McGlynn, C., Vera-Gray, F. (2024) 'Fake Porn, Real Victims We must stop the easy use of AI to create nude images of women & girls', link.

53. My Image, My Choice (2024) Deepfake Abuse Landscape Analysis: The exponential rise of deepfake abuse in 2023-2024, link.

54. ABC News (2023) 'Mobile apps fueling AI-generated nudes of young girls: Spanish police', link.

55. Internet Matters (2023) 'It's really easy to go down that path': Young people's experiences of online misogyny and image-based abuse, link.

56. Internet Matters (2019) Vulnerable Children in a Digital World, link.

57. Internet Matters (2020) Refuge and Risk Report: Life Online for Vulnerable Young People, link.

58. Internet Matters (2020) Look At Me: Teens, Sexting and Risks, link.

59. Internet Matters (2023) 'It's really easy to go down that path': Young people's experiences of online misogyny and image-based abuse, link.

60. Naezer, M., van Oosterhour, L. (2021) 'Only sluts love sexting: youth, sexual norms and non-consensual sharing of digital sexual images', Journal of Gender Studies 30, link.

61. Ringrose, J., Rehehr, K. (2023) 'Recognizing and addressing how gender shapes young people's experiences of image-based sexual harassment and abuse in educational settings', Journal of Social Issues, link.

62. Hanson, E., McGeeney, E. (2017) Digital Romance: A research project exploring young people's use of technology in their romantic relationships and love lives, link.

63. The Independent (2024) 'Spain court sentences 15 schoolchildren for spreading AI-generated naked images of classmates', link.

64. College of Policing (2016) Briefing note: Police action in response to youth produced sexual imagery ('Sexting'), link.

65. Department for Education (2024) 'What is the national curriculum and why is it being reviewed?' link.

66. Sky News (2024) 'Children to be taught how to spot fake news and 'putrid' conspiracy theories online in wake of riots', link.

67. My Image, My Choice (2024) Deepfake Abuse Landscape Analysis: The exponential rise of deepfake abuse in 2023-2024, link.

68. Metro (2024) 'Girl killed herself when bullies shared fake nudes of her', link.

69. Ministry of Justice (2024) 'Government cracks down on 'deepfakes' creation', link.

70. Labour Party (2024) Change: Labour Party Manifesto 2024, link.

71. Protection of Children Act 1978 and Coroners and Justice Act 2009, see CPS guidelines (link).

72. Ministry of Justice (2024) 'UK signs first international treaty addressing risks of artificial intelligence', link.

73. See proposals in Internet Watch Foundation (2024) One step ahead: A manifesto for tackling child sexual abuse online, link.

74. Morgan, N. (2023) 'On misogyny, the Online Safety Bill is still woefully inadequate', link.

75. Online Safety Act 2023, Section 54.

76. Ofcom (2023) Protecting people from illegal harms online: Volume 4 How to mitigate the risk of illegal harms – the illegal content Codes of Practice, link.

77. Ofcom (2023) Protecting people from illegal harms online: Volume 2 The causes and impacts of online harm, link.

78. National Police Chiefs' Council (2024) 'Child Sexual Abuse and Exploitation Analysis Launched', link.

79. Internet Matters (2024) Response to Ofcom consultation on the draft Illegal Harms code of practice, link.

80. Internet Matters (2024) Insights from Internet Matters tracker survey, link.

81. Internet Matters and Praesidio Safeguarding (2024) Shifting the dial: Methods to prevent 'self-generated' child sexual abuse among 11-13-year-olds, link.

82. Ofcom (2024) Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes, link.

83. MIT Technology Review (2024) 'Google is finally taking action to curb non-consensual deepfakes', link.

84. Internet Matters (2024) Insights from Internet Matters tracker survey, link.

85. Ofcom (2024) Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes, link.

86. Internet Matters (2024) A Vision for Media Literacy: Charting the path for media literacy in schools, link.

87. Internet Matters and Praesidio Safeguarding (2024) Shifting the dial: Methods to prevent 'self-generated' child sexual abuse among 11-13-year-olds, link.