**Ofcom: protecting people from illegal harms online**

**Internet Matters consultation response**

February 2024

About Internet Matters

**Internet Maters is a not-for-profit organisation dedicated to supporting parents and professionals to keep children safe and well online.** We are one of the most popular information sources among parents - in 2022/23 we received over 9 million visits to our site.

In addition to our expert guides and resources for parents and teachers, we also have a Policy and Research function.[1] We use our insights to **champion the views and interests of families**, making evidence-based recommendations to all those with influence over children's digital lives. This includes our industry partners as well as government, policymakers and parliamentarians.

Internet Maters is represented on the Government's Media Literacy Taskforce Steering Board and the Executive Board of the UK Council for Internet Safety (UKCIS), as well as Ofcom's Making Sense of Media Panel. We chair UKCIS's Vulnerable Users Working Group.

About this submission

Internet Maters is a **long-term advocate for greater online regulation**. We are delighted to offer the evidence below in support of Ofcom's approach to its new duties to protect users from illegal content under the Online Safety Act.

**We see children's online safety and wellbeing as a shared responsibility between service providers, Government and regulators, as well as parents and the professionals who support families and children** – for example teachers and social workers. Although it is shared, we think that **much more needs to be done to protect children by design**, i.e. by service providers.

The Online Safety Act is a landmark development in the journey to keep children safer online. Ultimately, we would like approaches to children's online safety to shift from a position of protection and restriction, to one where children of all ages can benefit from being online safely and confidently - independent regulation is a key plank for achieving this. **We welcome the speed with which Ofcom has assumed its new duties in the Act and there is much that is positive in this first draft code of practice**.

Alongside our work to support parents and professionals, we also conduct an extensive research programme. **From these insights we believe that there are a number of key areas in which Ofcom can improve the way it approaches its new duties relating to illegal harms**. This submission includes our latest evidence on children's experiences of illegal harms - as well as parents' concern and awareness of these issues - and we begin our submission (in response to Question 1) with more granular information of the risks to children of illegal content and behaviour.

[1] More about our data sources and underlying evidence for our response to this consultation is set out in answer to Q.1

**Summary of key points**

- **Experience of illegal harms by children is unfortunately widespread and commonplace, particularly for teenagers.** And a number of harms (such as being contacted by strangers) appear to more significantly impact on girls more than boys. For example, in response to a recent nationally-representative survey conducted by Internet Matters, **14% of teenagers under the age of 16 said they have experienced a form of image-based child sexual abuse**, **which is around 417,000 children in the UK**.[1] We understand Ofcom's inclination not to apply unnecessary burden to small and growing businesses, **however we believe that the level of illegal harm *already* experienced by children provides clear grounds to widen duties beyond those classified as 'large' or medium/high risk**. Children are often the earliest adopters of new platforms and services, and it is important for risk assessment and safety duties to be embedded at the earliest stages of governance and product development, given the speed at which online platforms can grow (taking principles of proportionality for small businesses from Health and Safety legislation). This will also protect against the risk of offenders migrating to smaller, unregulated platforms to conduct offences and to share illegal material, such as child sexual abuse material (CSAM).

- **We suggest that Ofcom takes a differentiated approach to child-on-child sexual abuse in the illegal harm Codes of Practice,** which recognises how the dynamics and risk factors underpinning this behaviour differ from adult-perpetrated CSEA. **A quarter (25%) of teenagers under the age of 16 are aware of a form of image-based abuse being perpetrated against another young person, which is approximately 745,000 children in the UK.[1]** Among teenagers who have experienced a form of image-based harassment or abuse (14% of those aged 13-16) **over half (55%) reported a known young person as the 'perpetrator', 22% an unknown young person, and a further 12% reported a current or former boyfriend or girlfriend**. But currently, child-on-child abuse is only mentioned twice in Ofcom's analysis of the causes and impacts of illegal harms, where it is subsumed into more general CSEA commentary, and not at all in the draft Code of Practice. Child-on-child abuse differs from adult-offending in terms of how it manifests, the risk factors, mitigations, and the appropriate responses to all children involved – we suggest that this is reflected in Ofcom's approach to regulation.

- We welcome requirements on large and risky services to implement hash-matching to detect known child sexual abuse material (CSAM) – i.e. material which is already recorded on a central database – and to remove it swiftly. However, use of hash-matching technology is an existing industry standard,[1] and there is a clear omission – in the current illegal harms Codes of Practice – around proactive steps to detect and remove new CSAM from circulation. **We recommend that Ofcom addresses this urgently as a priority – either in response to this round of consultation, or in future iterations of the illegal harm Codes of Practice – to require companies to test and implement technology to detect the sharing of new CSAM.**

- **Parents are key to protecting children from illegal harms**. Children who have experienced an online harm, including illegal harms, are far more likely to report their experience to a parent (48%) than to the platform (25%). For the illegal harms and wider online safety regulation to succeed, it is crucial that parents are integrated into each stage of children's online journeys, including if they experience illegal content or conduct. **It is disappointing to see the lack of any references to the role of parents and caregivers in the draft illegal harms Code of Practice**. **While it is important for terms of service to be accessible for children, we believe that more active consideration should be given to the role of parents.** For example, Ofcom could require large platforms to have an option allowing children to nominate a parent/caregiver to make reports/undergo redress on their behalf, a functionality which is already available and well-used across many large social networking platforms.[1]

| Question 1: | |
|---|---|
| i) | Do you have any comments on Ofcom's assessment of the causes and impacts of online harms? |

Background

Internet Matters conducts an extensive research programme which is designed to provide us with insight into families' experiences of digital platforms and technologies. **To inform our response to this consultation, we are drawing upon our two major data sources on the prevalence and impact of illegal online harms to provide more granular information on the online risks to children in particular**.

- We conduct a twice-yearly **'digital tracker survey'** with a nationally representative sample of over 2,000 parents and 1,000 children aged 9-16. We present child participants with a list of harmful experiences and ask them to select any harms that they have experienced and the impact that it had on them. We ask a corresponding question to parents, asking them which harms they believe that their child has experienced and the degree of impact – this allows us to make important comparisons between what children experience and what parents know and understand about those interactions.

- Our flagship **Digital Wellbeing Index** is an annual study designed to assess the impact of digital technology on children's lives – both positive and negative – and the factors which shape children's outcomes. The study is based on a four-dimensional framework of digital wellbeing (developmental, emotional, physical and social) developed in collaboration with the University of Leicester. Findings are based on a detailed household survey of 1,000 children and their parents.

We also conduct regular **deep dive research projects** on particular themes, including emerging tech (examples include the metaverse and cryptocurrencies) and thematic issues (examples include vulnerability, online misogyny and image-based abuse).

This response is structured in such a way to provide the best possible overview of our evidence relating to children's experience of illegal harms and the impact that illegal content and behaviour has on them, as well as the concerns and awareness of parents. In this response we set out our latest data on:

- **The prevalence of illegal harms** – our quantitative and qualitative evidence on children's experiences
- **The impact of illegal harms on children**
- **The experience of *vulnerable* children**

The prevalence of illegal online harms

**Quantitative evidence: illegal harm prevalence**

Across our tracker survey we ask children twice a year about their exposure to a number of online harms associated with illegal content or behaviour.[2] There are limitations in the extent to which we can assess whether individual experiences of harmful content amount to illegal harm (e.g. knowing whether self-harm content passes the threshold for illegality, or whether unsolicited contact by a stranger on an online service represents a grooming offence). We have bucketed data points under three priority offence areas – child sexual abuse and exploitation (CSEA), self-harm offences[3] and fraud offences.

Content/behaviour related to CSEA offences:

- Being contacted by strangers
- Sexual harassment and abuse from other children online
- Non-consensual image-sharing

Content/behaviour related to self-harm offences:

- Coming across content promoting self-harm

[2] Some of these are restricted by age to children aged 13 and above, given safeguarding considerations of the survey (which is conducted anonymously and not necessarily with adult supervision).
[3] Note that we ask parents about their child's exposure to suicide content, but do not do so on the children's survey

Content/behaviour related to fraud offences:

- Being tricked by stranger, or a stranger attempting to steal money
- Being asked to give away personal information

Some forms of harm are asked to children of all ages (9-17) – for example, being contacted by strangers and being tricked or asked to give away personal information – while some harms are restricted those aged 13 and above, such as self-harm content, receiving or sharing sexual images and sexual abuse from other children.

Being contacted by strangers online is the harm that children are by far the most likely to experience online, out of the 8 harms we survey: **over 1-in-5 (21%) children aged 9-16 report having experienced contact** this.

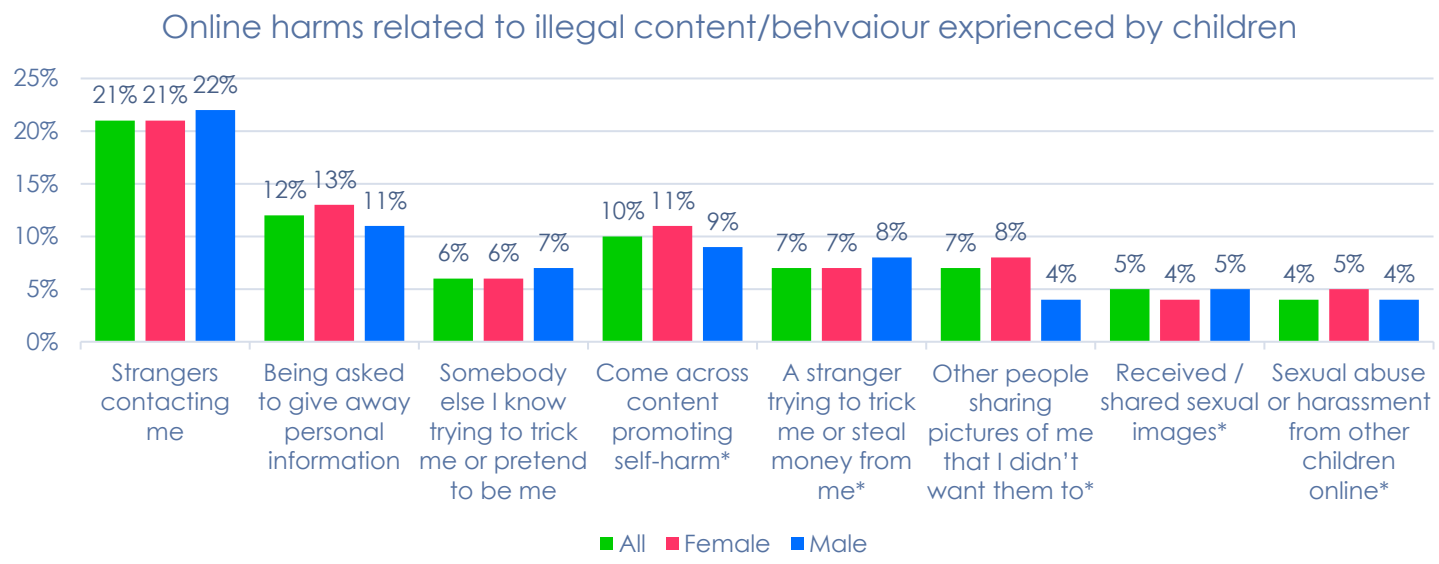



*Figure 1 – Answers to "Which of the following have you done or experienced online (in the past few weeks)?", nationally representative sample of over 1,000 children aged 9-17, November 2023 (questions marked * asked to children aged 13-17 only).*

We also see that the proportion of children who are contacted by strangers online increases sharply at age 13, from 18% of 11-12-year-olds, to a quarter (26%) of 13-14-year-olds, as illustrated in Figure 3.

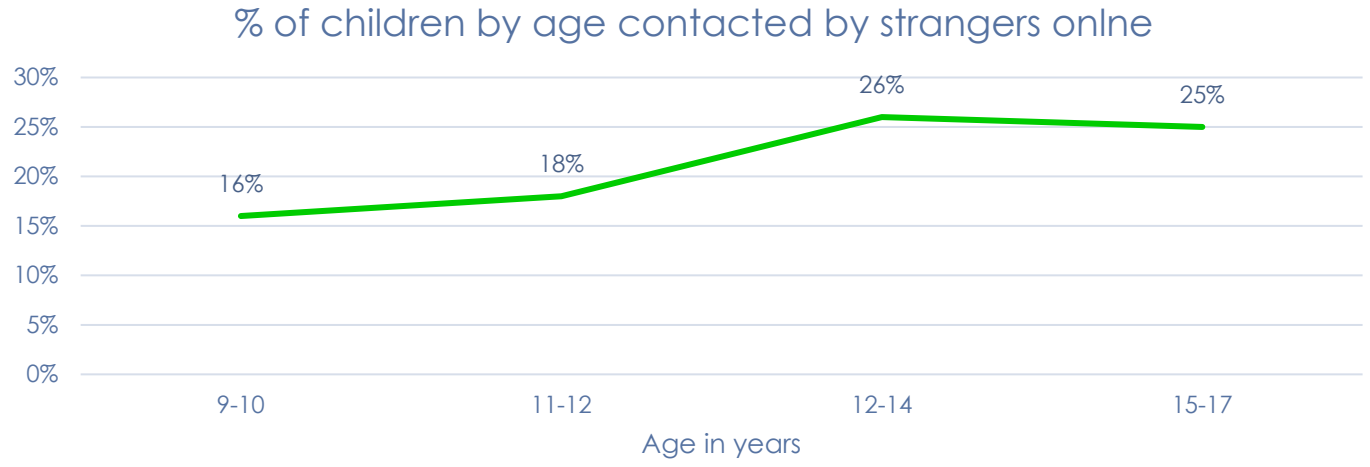



*Figure 2 - Children aged 9-17 who said that they have been contacted by strangers online, in the past few weeks (November 2023), by age group.*

What parents understand about children's experiences of illegal online harm

We also ask 2,000 parents (not necessarily of the same household) a corresponding set of questions about their children's experience of online harms. From this, we are able to draw comparisons around children's **actual experiences** of harmful content and parents' **awareness** of these incidents.

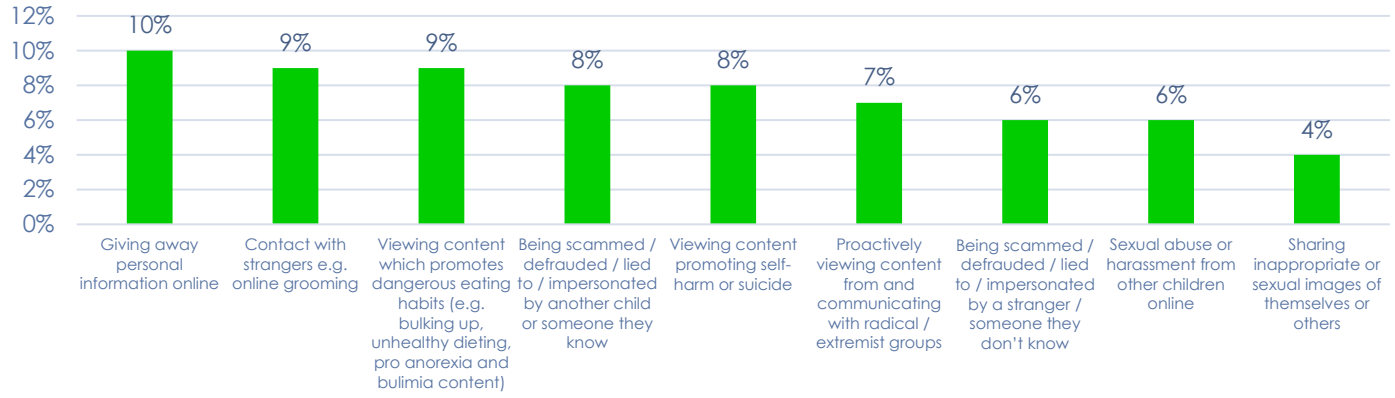



*Figure 3 - Percentage of parents (of children aged 4-17) who are aware of their child experiencing an online harm associated with illegal content or behaviour, November 2023. Ordered by percentage awareness among parents.*

Parents appear to underestimate the extent to which children are contacted by strangers online – **21% of children reported being contacted by strangers in the few weeks before the November 2023 survey, compared to just 9% of parents who reported awareness of this** (a significant 11-percentage point difference). Contact by strangers is by far the most frequent harm reported by children which is associated with illegal behaviour, but concerningly this is the harm that parents are most likely to underestimate. The lack of parental awareness unsolicited stranger contact online is likely to heighten the risk of these encounters.

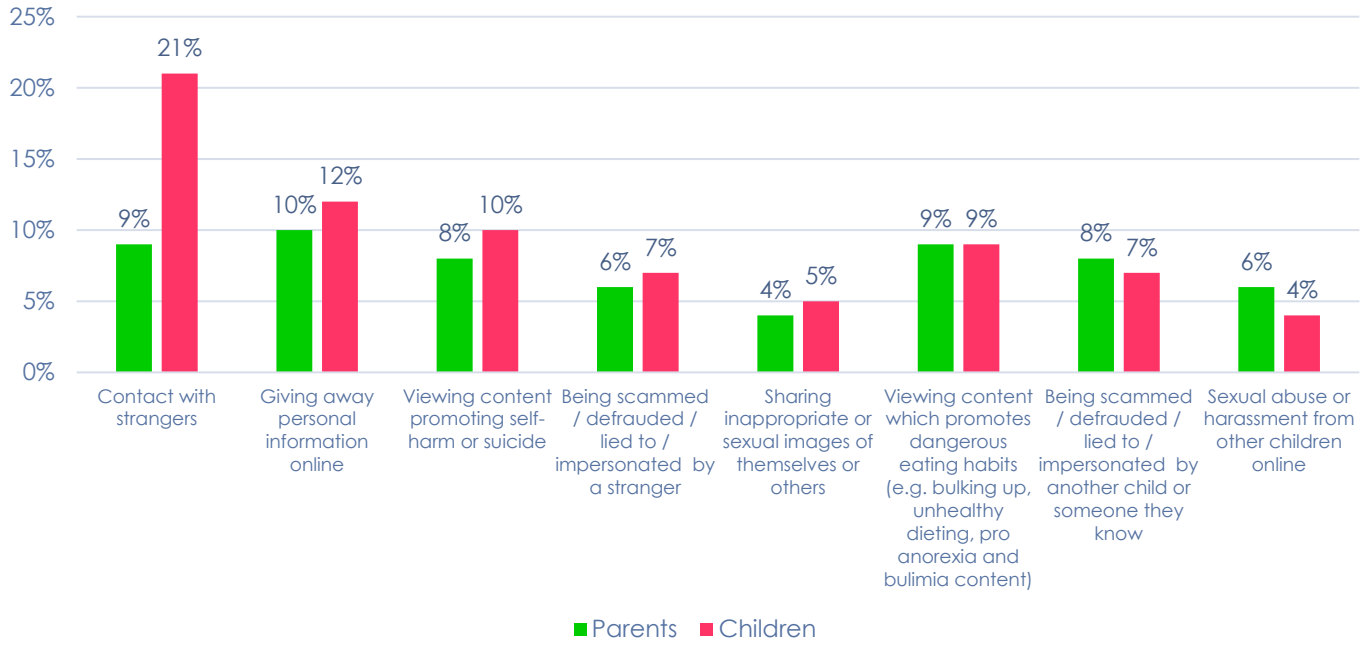



*Figure 4 - Awareness among parents (of children aged 4-17) and children (aged 9-17) of online harms associated with illegal content or behaviour, November 2023. Ordered by percentage difference between child and parent responses.*

Otherwise, we generally see alignment across children's reports and parental awareness around illegal harms, with variance consistently around 1-2% (notably there is a higher degree of variance in reports of legal but harmful content, which we will discuss in response to later consultations). Although it is notable that out of 8 categories of experience associated with illegal harms, **5 are reported more frequently by children than by parents**.

**Qualitative survey responses**

Across 2023 (over two survey waves conducted in May-June and November), a total of 494 children (aged 9-17) provided free-text responses on 'something that had concerned or bothered' them about being online in the past few weeks. As in previous survey waves, the majority of children shared experiences of legal harms (i.e. primary priority and priority harms to children), such as exposure to pornography, violent content, mis-/disinformation and technology-facilitated bullying.[4]

However, a number of responses point to exposure to potentially illegal content and behaviour, such as unsolicited contact from strangers online (a possible indication of attempted / early-stage grooming), non-consensual image-sharing and exposure to suicide and self-harm content.

Notably, 19 out of 24 children who wrote about experience unsolicited contact by strangers online were girls, which is supportive wider research on the gendered nature of unsolicited online contact, grooming and CSE.[5] Internet Matters will be publishing specific research into the experience of girls online next month, which includes a focus on harassment.

Examples of free-text responses about unsolicited contact from strangers include:

> "*I keep getting messages from guys I don't know, and they ask me where do I live, I don't tell them and block them but I still get msgs from them on another account*" – Girl, 11.
>
> "*somebody asked me to send my boobies but i blocked them and told mum*" – Girl 13.
>
> "*Random people adding me to groups and asking to do things sexually*" – Girl, 15.

A number of children, aged 13-16, wrote about harmful experiences of non-consensual image-sharing. It isn't possible to determine – from these responses – the nature of the pictures involved (i.e. whether they involve nudity or would be classified as CSAM), but words such as 'threaten' and 'consent' may be indicative of a sexual element.

> "*Threaten photographs on instagram of me from years ago*" – Girl, 13
>
> "*People uploading video of me without my consent*" – Girl, 16.
>
> "*Not me but my younger sis, someone screenshot her snaps so I confronted the boy at school and asked him to delete*" – Boy, 16

We also received a number of responses about exposure to content, language and behaviour relating to self-harm and suicide, from children as young as 9:

> "*Talking about suicide*" – Girl, 9
>
> "*The level of self harm content*" – Girl, 13
>
> "*Violence and suicide chat*" – Boy, 14

All quotes above are in response to the survey question '*Please tell us about anything that has concerned or bothered you about being online in the past few weeks? This could be anything that you have read or seen online*' – asked to children aged 9-17 in May-June and November 2023.

[4] More detail on qualitative responses on (primary) priority harms to children will be shared in later consultation responses where relevant.
[5] For example, Internet Matters (2024) 'Children's Wellbeing in a Digital World: Year Three Index Report 2024'. Link, which finds that almost half (48%) of teenage girls have been contacted by a stranger – up from 29% in the previous wave.

The impact of illegal harms on children

Our regular tracker survey asks children to rate the effect that it had on them – on a scale of 1 to 7, where 1 is no impact and 7 is a significant impact.

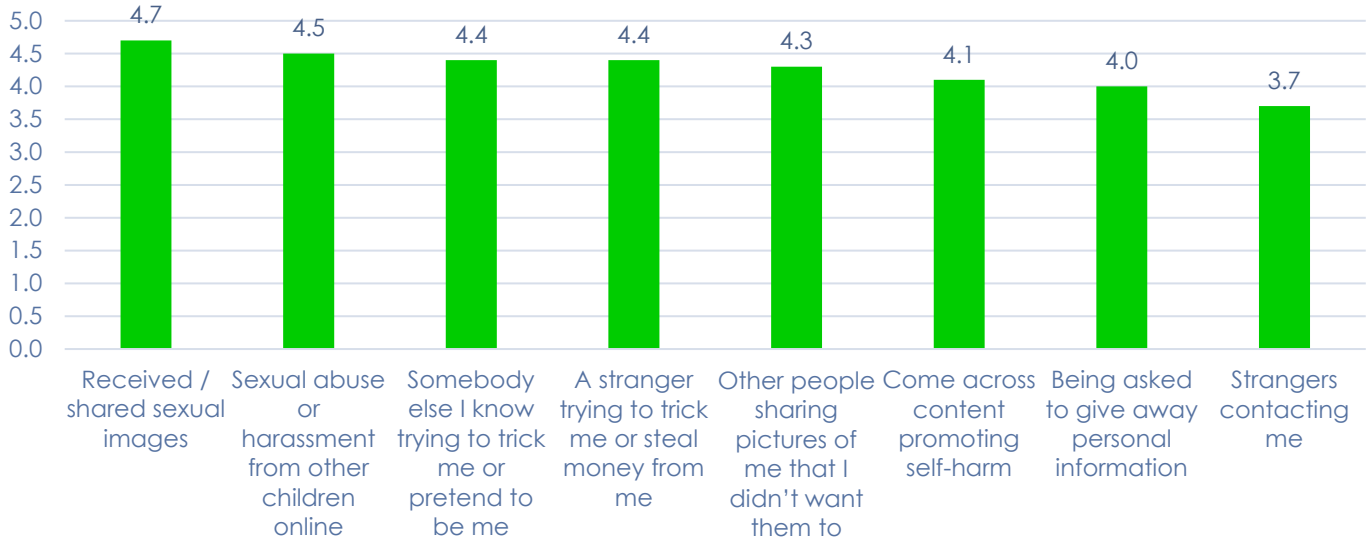



*Figure 5 - Self-reported impact of online harms associated with illegal content/behaviour (scores out of 7), nat-rep sample of 1,000 children aged 9-17, November 2023.*

All nine categories of harm that we have classified as indicative of illegal content or behaviour have an impact on children. However, there is a 1-point degree of difference between the children's self-reports of the highest impact harm (receiving and sharing sexual images – 4.7/7 severity) and the lowest (strangers contacting me – 3.7/7 severity). It is worth noting that the harms which appear to have the greatest impact on children are those which ostensibly contain a sexual element; receiving or sharing sexual images, and sexual harassment /abuse from other children scoring highest in terms of self-reported impact on children**. This underscores the need for the illegal harms Codes of Practice to tackle child-on-child sexual harassment and abuse**, among other important areas, as discussed in response to **Q.16**.

We find that age plays a significant factor in children's experience of illegal harms, with younger children generally reporting a more significant impact from exposure to harms. This will be – at least partly – due to developmental factors and a greater ability to deal with challenging content at older ages, but **desensitisation** (e.g. being contacted by strangers becoming 'commonplace' and even normalised among older groups) is likely to also play a part, as highlighted in our forthcoming research on the online lives of teenage girls.

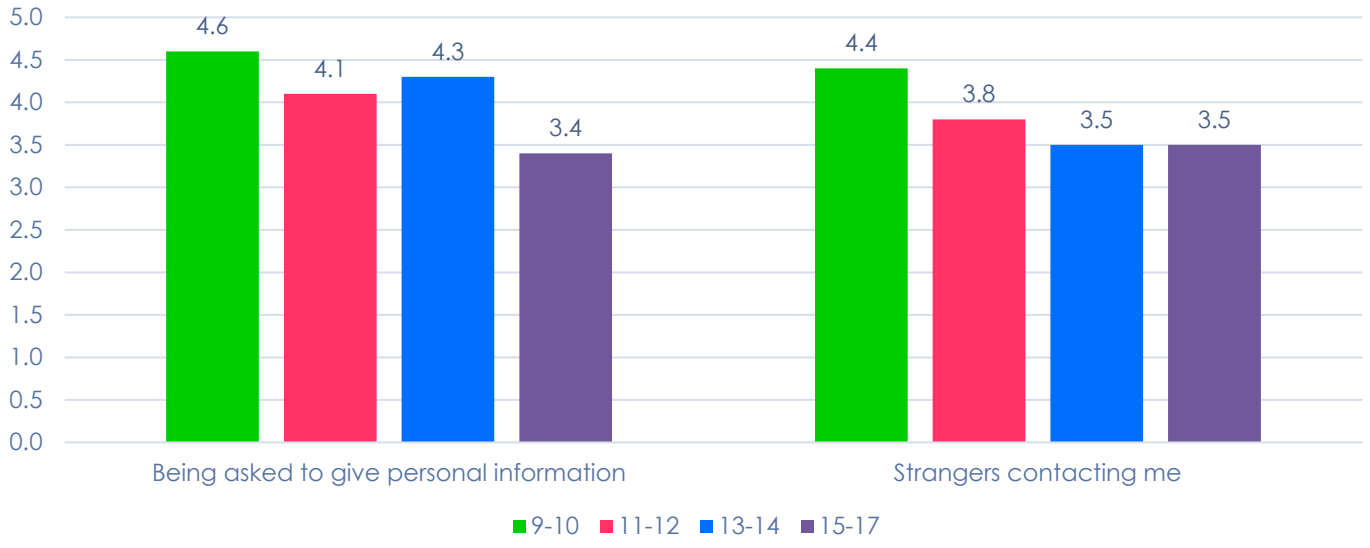



*Figure 6 - Self-reported impact of online harms, on scale of 1-7, by children's age (November 2023)*

Girls also generally report more significant impacts of some illegal harms that boys – this is likely to be, at least in part, due to a higher likelihood of experiencing more serious harmful content and behaviour. In particular, girls reported a more significant impact following exposure to self-harm content (22% difference in higher self-reported impact), dangerous eating habits (22% difference in higher self-reported impact) and child-on-child sexual harassment or abuse (16% difference in higher self-reported impact).


*Figure 7 - Self-reported impact of illegal harms (on scale of 1-7) with greatest difference between boys and girls, children aged 13-16, (November 2023)*

The experience of vulnerable children

Internet Matters' research consistently indicates that children with vulnerable 'offline' circumstances – for example, children in social care, with special educational needs (SEN) or disabilities, and children with mental health needs – are more likely to experience harms in the online world.[6] To understand this in more depth, our regular tracking survey contains a subset of vulnerable children who – for the purposes of the survey – we define as children:

- Who receive special education needs (SEN) support and/or,
- Who have an Education, Health and Care Plan (EHCP), indicating a significant level of SEND, and/or,
- Who have a mental or physical health need which requires professional support.

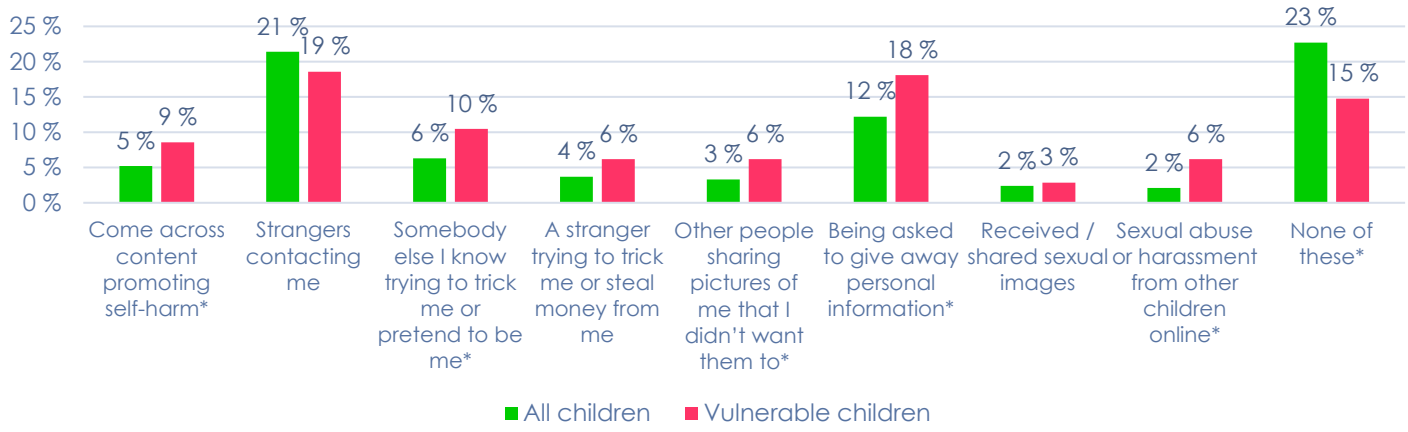



*Figure 8 - Answers to "Which of the following have you done or experienced online (in the past few weeks)?", nationally representative sample of over 1,000 children aged 9-17, November 2023, by vulnerability.* ***Harms marked * are statistically significantly different.***

With the exception of being contacted by strangers, **we find that vulnerable children are more likely to experience every online harm surveyed which may be related to illegal content or behaviour**. We can also see that vulnerable children are statistically significantly more likely to experience a range of harms including coming across content that promotes self-harm, someone else they know trying to trick them or pretend to be them, others sharing pictures of them they didn't want shared, being asked to give away personal information and sexual abuse or harassment from other children online. **Vulnerable children are also statistically significantly less likely to have not experienced an online harm associated with illegal content or behaviour**.

We also find that vulnerable children are more likely to experience more significant impacts from experience of 6 out of 9 online harms associated with illegal content or behaviour.

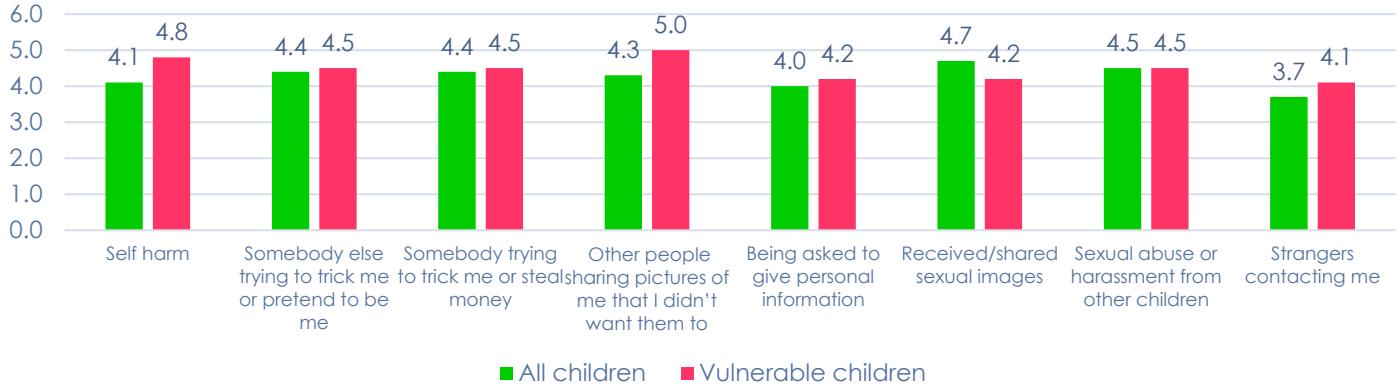



*Figure 9 - self-reported impact of experiencing online harms associated with illegal content/behaviour, children aged 9-16, November 2023, by vulnerability*

[6] For example, Internet Matters (2021), 'Refuge and Risk: Life online for vulnerable children'. Link.

| ii) Is this response confidential? (if yes, please specify which part(s) are confidential) |
| --- |
| Response: No |

| Question 13: | |
|---|---|
| i) | Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk? |
| Response: No | |
| ii) | Please provide the underlying arguments and evidence that support your views. |

There is clear evidence that small platforms and services are liable to pose a high risk to children of experiencing illegal content (such as serious suicide and pro-self-harm material) and being victim to illegal conduct (such as grooming and CSAM distribution).[7] It is also well known that different stages of illegal conduct are often conducted across multiple platform types. For example, as set out in Volume 2,[8] child grooming offences often originate on large platforms, such as social media and gaming platforms, where offenders have access to a large number of children, before migrating to smaller services to commit abuse and/or distribute illegal material such as CSAM.

It is critical that small services are not exempt from duties to protect users - particularly children - from illegal content. The current approach risks accelerating the process of multi-platform offences, resulting in illegal content being displaced across smaller services - where offenders can exploit the fact that governance and content moderation processes are not placed to proactively identify and take action against illegal conduct.

We suggest that Ofcom take the same approach to illegal duties as health and safety policy where, generally speaking, health and safety laws apply to all businesses - regardless of size and/or risk profile.[9] It is generally recognised that responsibility for health and safety doesn't have to be complicated, and the approach for small and low-risk businesses can be straightforward and proportionate.[10] Compliance with risk assessment and governance duties – particularly those which protect children from the most serious illegal harms, such as CSEA – do not need to necessitate heavy cost burdens or disproportionate 'inconvenience' to users (as suggested by Ofcom's rationale for excluding small and 'low-risk' services from certain duties).[11]

At the very least, we recommend that Ofcom requires companies of all size and risk profile to:

- **Comply with robust illegal content risk assessment proposals**, including undertaking annual reviews of risk management.[12]
- **Comply with full governance proposals**, to ensure that sufficient structures are in place to identify and act on emerging/evolving risks.[13]
- **Comply with full content moderation duties**, for example duties to have content policies and performance targets, to ensure that small/single risk services quickly identify emerging risks and illegal content/behaviour.[14]

We do not believe that the all of above measures - if applied and regulated proportionately - will represent 'overbearing' regulation for smaller platforms. Given the speed with which small platforms can grow and reach a high number of users (in a matter of weeks or months) - particularly among child users, who are often the first adopters of new platforms and technologies. It is important that risk management and content moderation are embedded into the earliest stages of platform development and service governance.

In addition, it would be positive for a greater number of platforms to be required to:

- **Implement hash-matching of user-generated content to detect CSAM**, given the severity of harm associated with image-based CSAM, we disagree with Ofcom's assessment that it is disproportionate to require platforms which enable user-generated content sharing to deploy hash-matching. [15]

As Ofcom notes in its own analysis of the risk-factors associated with CSAM-sharing, intelligence suggests that offenders seek out smaller and less-mature services to procure and distribute CSAM – in the knowledge that

[7] For example, as set out by Ofcom, (2023), Illegal Harms consultation Volume 2, 6C.143 – 'intelligence suggests that perpetrators often seek out services with smaller user bases, particularly services that are less mature, as these services may have fewer CSAM detection technologies or processes in place.'
[8] Ofcom (2023) Illegal harms consultation Volume 2, 6C.41. Link.
[9] Health and Safety Executive, 'Simple health and safety policy'. Link.
[10] Companies House, 'Health and safety basics for your business'. Link.
[11] Ofcom (2024) 'Why size and risk matter in our approach to online safety'. Link.
[12] Ofcom (2023) Illegal harms consultation Volume 3, 8.45. Link.
[13] Ofcom (2023) Illegal harms consultation Volume 3, 8.35. Link.
[14] Ofcom (2023) Illegal harms consultation Volume 4, 12.116. Link.
[15] Ofcom, 2023, Illegal harms consultation Volume 4, 14.106. Link.

fewer detection measures are in place. Despite the costs associated with CSAM-detection tools (such as hash-matching) – we do not believe that this is disproportionate to the benefit of removing CSAM on a service which is being used to distribute it, given the immense and lasting harm that CSAM causes to victims.

| iii) Is this response confidential? (if yes, please specify which part(s) are confidential) |
| --- |
| Response: No |

| Question 16: | |
|---|---|
| i) | Do you have any comments on the draft Codes of Practice themselves? |

Yes. We have structured our response to this question under key thematic headings, where we have suggestions for improvement to the draft Codes of Practice: **child-on-child abuse**; **detection of previously-undetected CSAM**; and protecting children from **pro-suicide and self-harm content**.

## Child-on-child sexual abuse

### Background

Adolescent and teenage intimate relationships are now initiated and developed in online spaces, as fluidly as they do in 'offline' contexts. Technologies are used, for example, by young people to meet new partners, flirt, communicate, share intimate images, and break-up – with many affordances of technology in intimate relationships being seen positively by young people.[16]

However, it is well-known that each of these behaviours is associated with risk. And it is well-documented that technology can also be used by children and teenagers to commit sexual harassment and abuse against other young people. There are various categories of child-perpetrated sexual violence which can manifest online, including:[17]

- Online sexual harassment – e.g., unwanted sexual comments, pressure to share sexual content
- Image-based harassment – e.g., 'cyberflashing'
- Image-based abuse – e.g., non-consensual sharing of sexual images, threats and blackmail associated with sexual images
- Gender- or sexuality-based hate speech

Online child-on-child abuse is a considerable issue that impacts on both victims and young people who perpetrate sexual abuse, as well as their families. It has become increasingly difficult for schools to safeguard children from child-on-child abuse, where it is perpetrated online (particularly when outside school hours). This fact was highlighted by a 2021 Ofsted review into child-on-child sexual abuse, which found that 90% of girls have been sent explicit pictures that they didn't want to see, and that 'professionals consistently underestimated the prevalence of online sexual abuse'.[18]

### Evidence of scale and impact

Overall, it is estimated that anywhere between one-fifth to two-thirds of all child sexual abuse (online and off) is committed by other children and adolescents.[19] It is hard to establish an accurate estimate of the proportion of child-on-child sexual offences – given chronic issues of under-reporting by victims and more lenient policing/sentencing approaches to child suspects and offenders, particularly in recent years.[20] Many experts suggest that an estimate of 'around a third' of child sexual abuse being perpetrated by other children is a sensible best guess.[21]

It is even harder to reliably estimate the scale of child-on-child abuse perpetrated online or with use of digital technologies, given issues around reporting and disclosure – particularly among male victims. However, Internet Matters research into the prevalence of image-based harassment and abuse (quantitative fieldwork conducted May-June 2023 and qualitative fieldwork in August 2023) indicates the following:

- **14% of teenagers aged 13-16 reported having experienced a form of image-based harassment or abuse**. This is likely to be a low-bar estimate – given the complexities around disclosure of sexual abuse, particularly for boys.

---

[16] McGeeney, E., & Hanson, E. (2017). Digital Romance: The centrality and affordances of technology in young people's relationships and love-lives. *Brook & CEOP*. Link.
[17] We base this categorisation on work by Henry, N. and Powell, A. (2014) to establish the range of sexually aggressive behaviours perpetrated with digital technologies, source.
[18] Ofsted, (2021). Review of sexual abuse in schools and colleges. Link.
[19] Hackett, S. (2014). 'Children and young people with harmful sexual behaviour: Research Review', *Research in practice*. See p.15 for overview of challenges in reliably establishing this figure. Link.
[20] E.g., following the introduction of police Outcome 21 for youth-produced sexual imagery cases. Outcome 21 is intended to respond to 'non-aggravated' indecent image cases (i.e. those which do not contain abusive behaviours), but there are concerns that overuse by officers (driven by lack of confidence and training) has concealed the true scale of abusive image-sharing incidents between children. Source: College of Policing, 'GD8 – Youth Produced Sexual Imagery - Guidance for Disclosure', Link.
[21] NSPCC (2021) 'Statistics briefing: child sexual abuse'. Link.

- The majority of teenagers who have personal experience of a form of image-based harassment or abuse report that **another young person was the perpetrator of this behaviour**. **Among children who have experienced non-consensual image-generation or distribution, over half (55%) reported that another young person was the perpetrator**. **A further 12% report their current or former boyfriend or girlfriend** – who is likely (although not necessarily) to be another young person – **and 22% an unknown young person**. This is compared to 10% who reported a known adult as the perpetrator, and 29% who reported the perpetrator as an unknown adult.

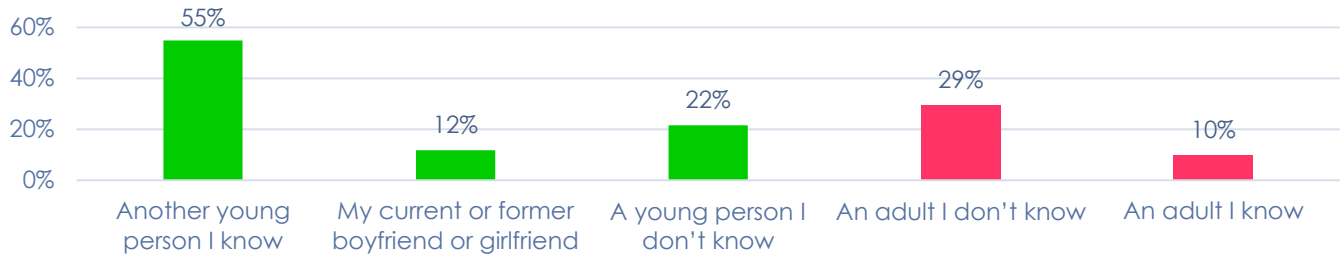



*Figure 10 – Reported perpetrators of image-based harassment and abuse, YOUNG PEOPLE and ADULTS, (cyberflashing, non-consensual nude image generation and distribution) – among teenagers with experience of image-based abuse aged 13-16 (May-June 2023)*

  - **Among children who have experienced threats associated with a nude image, 38% reported that this was perpetrated by another young person known to them** and a further **31% reported the perpetrator to be a current or former boyfriend or girlfriend** (compared to 8% who reported a known adult as the perpetrator).

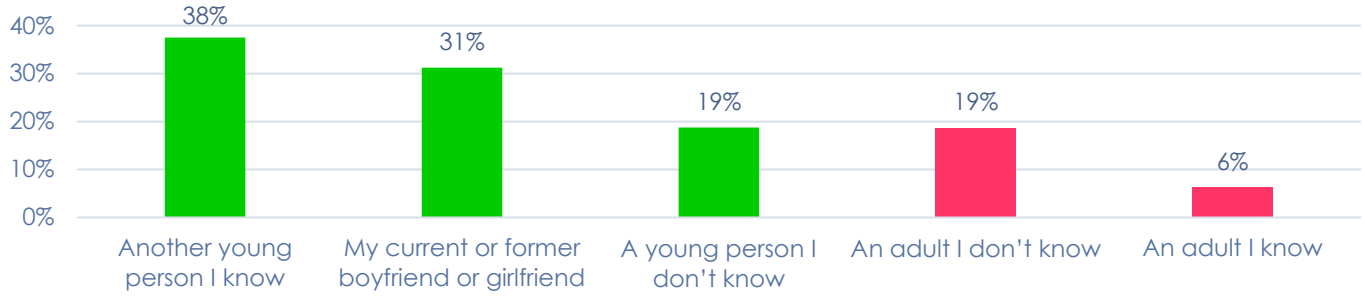



*Figure 11 - Perpetrators of threats associated with nude images YOUNG PEOPLE and ADULTS – among teenagers aged 13-16 (May-June 2023)*

- **A quarter (25%) of teenagers aged 13-16 are aware of a form of image-based harassment or abuse being perpetrated against another young person**. Again, this is likely to be an under-estimate, given sensitives of disclosure via an online survey. The most common form of image-based harassment or abuse known about by children is being sent unwanted sexual imagery (14%), followed closely by threats associated with sexual imagery (10%), non-consensual taking of sexual images (9%), non-consensual sharing of sexual images (8%) and deepfake nude images (8%).

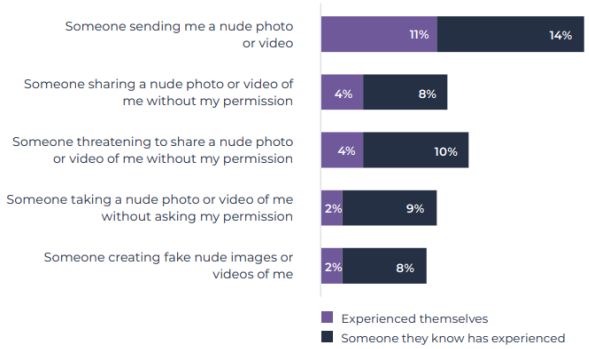
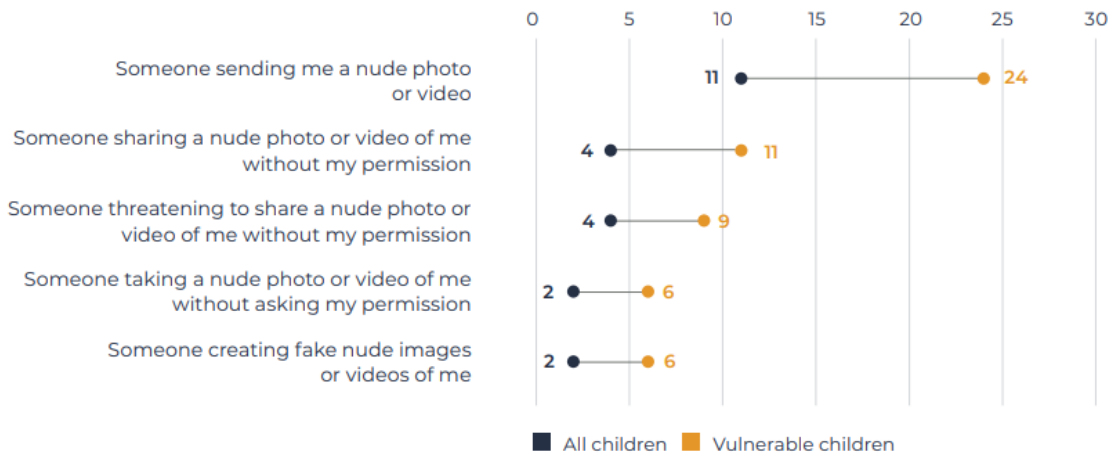



*Figure 12 - Experiences of IBSHA among young people aged 13-16 - personal or other known young people. Internet Matters May-June 2023.*

- **Vulnerable children[22] are significantly more likely to experience every form of image-based harassment and abuse** questioned in our survey.




In focus groups with teenagers aged 15-17, conducted separately with male and with female and non-binary teenagers, participants spoke about the pressures and harmful dynamics associated with nude images. Key themes included:

- Teenage girls spoke about a sense of 'ownership' that some male peers assume they have towards girls' nude images, and participants made a connection to misogynistic communities that boys are increasingly exposed to online: "*In one of [Andrew] Tate's quotes it says how men owned women, so they [young men/boys] could get into the mindset that because they own them they have the right to share a picture of them*." – Girl, aged 16-17.

- Teenage girls described nude-sharing as an almost 'standard' feature of intimate relationships – and suggested that denying a sexual image in a relationship could result in threats and aggression from male partners: "[Refusing to share a nude can be] *quite a big deal. If you're dating they think you owe them the nude or something*." – Girl, aged 16-17.

- Whereas boys tended to play down the seriousness of nude-image sharing. For example, one boy said: "*It's not the worst thing in the world to do, so long as [the recipient] they're trusted, but certainly not really, really young or anything like that*." – Boy, aged 17.

- Boys and girls both appreciated that the implications for nude-sharing (particularly 'leaks' of nude images) were more serious for girls, and the fall-out had a disproportionate impact on girls (as compared to boys, where an incident could more easily be 'laughed off').[23]

**Implications for the draft Code of Practice**

Given the clear evidence of the scale and impact of child-on-child abuse, which is likely to account for a sizeable proportion – if not the majority – of online CSEA offences, it is unfortunate that references to child-on-child abuse are only made in **twice** passing in Volume 2 ('The causes and impacts of online harm'),[24] and **not at all** in Volume 4 (the draft Codes of Practice) of the illegal harms consultation documents.

A nuanced approach to child-on-child abuse – separate from actions to tackle adult-on-child CSEA– is needed for a number of important reasons:

- **The dynamics of child-on-child sexual abuse are different from adult offending and, thus, the measures needed to combat it are related but distinct**. For example, it is common for the victim and 'perpetrator' of online child-on-child abuse offences to be known to each other in 'real life' (for example, at school or college) and to have peers or mutual connections in common. This is different to adult-on-child

[22] Here we define vulnerable children as those with a special education need or disability (SEND) in receipt of an EHCP and young people with a diagnosed mental or physical health need requiring professional support.
[23] For more detail see Internet Matters (2023), *'It's really easy to go down that path': Young people's experiences of online misogyny and image-based abuse*. Link.
[24] A total of two references to child-on-child sexual abuse are made in Volume 2 ('The causes and impacts of online harms'), 6C.4-5, where it is noted that 'the perpetrators of CSEA can themselves be children'.

online grooming – for example – where it is likely that the victim and perpetrator are unknown to each other in real life.

- **Responses to child 'perpetrators' of online sexual abuse will also be different from responses to adult offenders**. All children involved in child-on-child sexual offences should be adequately safeguarded, and (with particular consideration for the individual child's age, needs and developmental stage) referrals should be made for children who display harmful sexual behaviour – both for their own wellbeing and to prevent further harm.

- **Compared to adult-perpetrated CSEA, other children are more likely to be witnesses** (or at least to be aware of) child-on-child sexual abuse, including sexual bullying, harassment and non-consensual image-sharing.

**We recommend that Ofcom takes a differentiated approach to child-on-child sexual abuse, rather than simply subsuming it within duties to tackle adult-on-child CSEA**. This section of the Code of Practice should require platforms to recognise how the dynamics and impacts of child-on-child abuse differ from adult offending. The Code should include measures for platforms to take to ensure that all children involved are safeguarded (i.e. child victim(s), child perpetrator(s) and child witness(es) – noting the limitations of this language when applied to child-on-child offences).

Measures specific to tackling child-on-child sexual abuse may include:

- **Mandatory peer-reporting tools on children's accounts** to enable children to safely and confidentially alert a platform to child-on-child sexual abuse, such as the non-consensual sharing of nude images on a group chat. This should be accompanied by clear information for children and parents on how these tools operate – including that they will remain anonymous to peers following a report.

- **Reporting mechanisms for non-users such as parents and teachers**, who have been alerted to child-on-child abuse.

- **Preventative safety tools for child users**, such as prevention messages and advice when a messaging platform detects that a child is attempting to share a nude image with another user.[25]

**<u>Detection of new child sexual abuse material (CSAM)</u>**

Proposals to mandate use of hash-matching technologies to detect known child sexual abuse material (CSAM) are welcome, and a necessary step to ensure standards around CSAM detection are levelled embedded across industry. However, it is worth noting that hash-matching technology is an existing industry standard tool and is already deployed on a voluntary basis by most major user-to-user platforms in non-end-to-end encrypted environments.[26]

**As an urgent priority, we would like to see Ofcom take a step further in tackling CSE/A with measures to detect <u>new, previously undetected</u> CSAM**. We understand that Ofcom hasn't yet established an evidence base on the costs of classifier technology, given that its information powers came into force with the passage of the Online Safety Act in October 2023. However, many platforms are already deploying this technology – it is unclear whether there will be an incentive for companies to continue investing in, and innovating, if evidence of them doing so will be used to justify increasing the bar for compliance. We urge Ofcom to address this issue, and increase the bar as a matter of urgency, either following this round of consultation on the draft proposals – or within further iterations of the Codes of Practice, when more information is available to them.

| i) Is this response confidential? (if yes, please specify which part(s) are confidential) |
|---|
| Response: No |

[25] Note that Internet Matters is conducting research to build evidence around effective prevention messages and interventions (including digital interventions), with support from Nominet. Findings will be published in Spring 2024.
[26] National Centre for Missing and Exploited Children (NCMEC), (2022), *CyberTipline 2022 Report*. Link.

| Question 28: | |
|---|---|
| i) | Do you agree with our proposals? |
| Response: In part | |
| ii) | Please provide the underlying arguments and evidence that support your views. |

It is noted in Volume 4 (the draft illegal harms Codes of Practice) that Ofcom's behavioural insights research suggests that children do not always make appropriate complaints about online harms.[27] This is supported by Internet Matters' own research (fieldwork conducted November 2023) that finds, **among children who have experienced at least one online harm, only a quarter took action by reporting it to the platform**. **This is far outstripped by the number who spoke to a parent (48%).** In addition, just over a quarter (26%) of children said that their parent took action on their behalf.

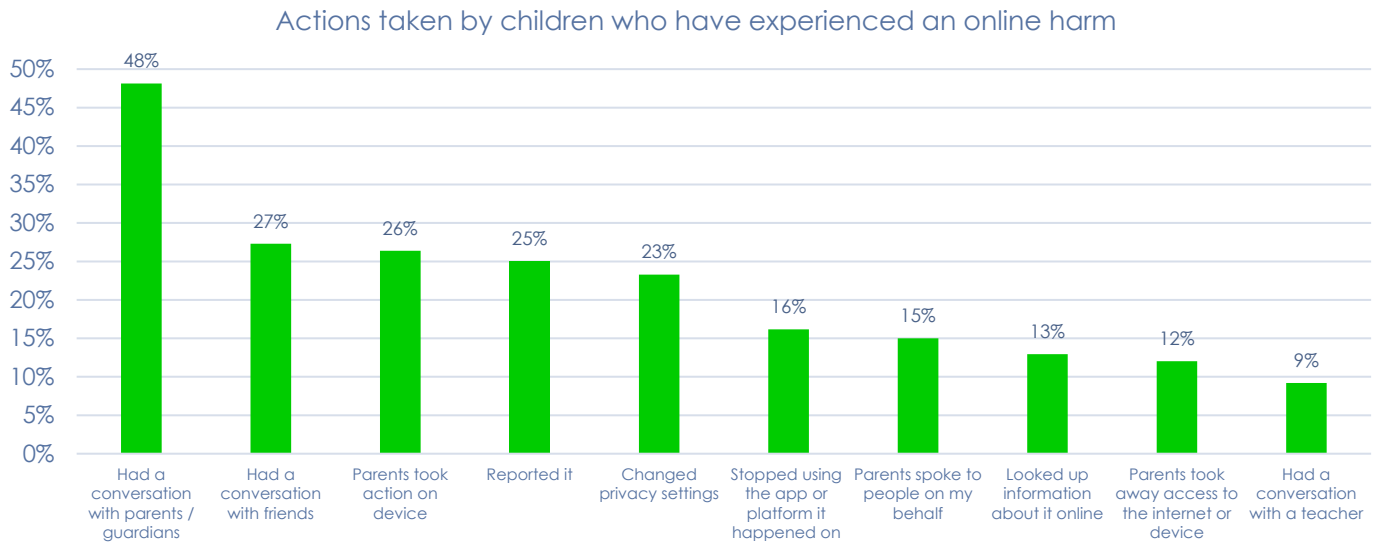



*Figure 13 - Actions taken by children who have experienced an online harm, children aged 9-16, November 2023*

Our data show that parental involvement is particularly important for younger children. Over half (56%) of children aged 9-10 spoke to a parent following experience of an online harm, compared to 40% of those aged 15-17.

Active involvement by parents may not be suitable for every child, and it is important that all children are given the resource and information to make complaints and reports independently. However, a formalised role for parents in the user-reporting and complaints duties would be hugely supportive for the majority.

To achieve this, Ofcom could consider requiring platforms to have:

- Child-friendly terms of service and reporting portals which include advice to speak to their parents about what they have experienced.
- Parent-friendly terms of service to support these conversations.
- An option for children to nominate a parent or caregiver to make reports on their behalf.

We recognise that not all children have parents or caregivers with the capacity to support them with online issues. Therefore, it is important for Ofcom to also consider requiring platforms to direct children to speak to their parents **or another trusted adult, such as a teacher**.

| i) | Is this response confidential? (if yes, please specify which part(s) are confidential) |
|---|---|
| Response: No | |

[27] Ofcom (2023), Illegal harms consultation Volume 4 16.49. Link.