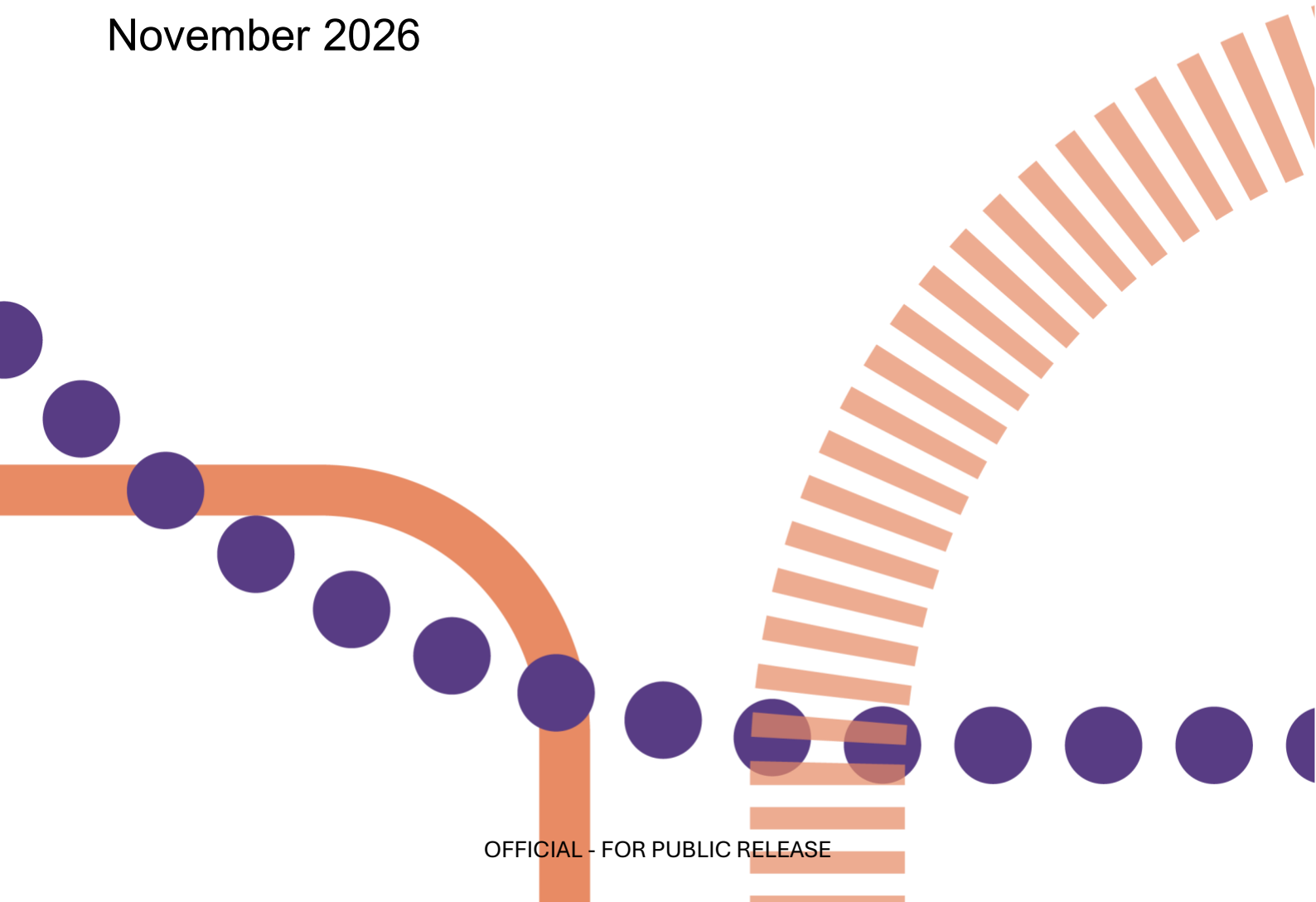
THE CHILD **SAFEGUARDING**
PRACTICE REVIEW PANEL

Safeguarding children from online harms

Online harms as a growing safeguarding risk

November 2026



Introduction

The Child Safeguarding Practice Review Panel recently welcomed and responded to Growing up in the online world: a national consultation and supports the Government's ambition to ensure children's experiences online are as safe, supportive, and developmentally appropriate as possible.

The Panel recognises the importance of ensuring that all children and young people can access and benefit from technology. It also hopes that the consultation will result in appropriate safeguards to ensure that access is suitable for children's age and the content they encounter.

> *"The online world is real, and the harm experienced there is real. Children need to be protected and supported within that world, not simply expected to leave it."*
>
> Parent of a child who experienced online harms

The Panel also recognises the importance of supporting practitioners, who often report feeling less confident navigating children's digital lives than assessing risk in physical settings. As children's lives become increasingly digital, safeguarding practice must continue to evolve. Providers also have a clear responsibility to improve the technical safeguards available to children. Strengthening practitioners' confidence and capability to assess digital safety and recognising that children may use largely unsupervised online environments, will be increasingly important to effective safeguarding practice. Routine enquiry about online activity and potential harm should form part of everyday safeguarding practice. Many local partnerships have already developed strategies in this area, and the Panel hopes these resources will support local work and contribute to national safeguarding improvement.

From the Panel's oversight of serious safeguarding incidents, there is growing evidence that online environments increasingly feature within the context of serious harm to children and young people. Online activity is rarely the sole driver of harm. Rather, it most often acts to facilitate, accelerate or intensify existing vulnerabilities, shaping how harm develops and escalates.

Online harm can also be cumulative. Seemingly separate experiences, including harmful content, bullying, coercion, sexual abuse, intra-familial harm and peer conflict, may interact and intensify over time. Understanding the child's online and offline experiences together is therefore essential to identifying an escalating pattern of risk.

A consistent theme across the Panel's learning is that online harm is not always recognised or understood early enough. In many cases, the challenge is not only responding to harm, but identifying it promptly, particularly when it occurs in online environments.

Serious harm can occur in unseen digital spaces, and safeguarding practice must routinely include active enquiry about and exploration of children's online lives, relationships, and behaviours, supported by strong multi-agency communication and professional confidence in addressing online risk.

Alongside the safeguarding responsibilities of practitioners and agencies, online services have an important role in protecting children. Under the UK's Online Safety Act 2023, services within scope must take steps to address illegal content and activity, including offences relating to child sexual abuse and exploitation, and fulfil duties to protect child users. Ofcom, as the independent regulator, oversees compliance with these requirements.

Online harm should not be understood solely as harm occurring outside the family home. Digital technology may also facilitate or compound intra-familial abuse, including through sexualised communication, image sharing, coercion, surveillance or continued contact with a child. Online harm may span all aspects of a child's life, inside and outside the home, and may involve people known to the child in person or only through online contact. Its reach can be global, enabling individuals and networks to access children across geographical boundaries.

This paper does not seek to address every form of online harm affecting children and young people. It focuses on learning from serious safeguarding incidents considered by the Panel, while recognising wider concerns relating to online communities, gaming platforms, harmful content, radicalisation and violence-focused online networks. Although these wider issues sit outside the paper's scope, some are subject to wider national consideration, including through the Southport Inquiry. Further briefings will be developed over time to help local partnerships navigate these complex issues.

Who is this document for?

Multi-agency practitioners and managers working in universal services such as schools, colleges, further and higher institutions, health services, police, and social care settings as well as relevant voluntary organisations and services working with adolescents.

How to use this resource

Multi-agency practitioners should use this resource as a practical guide to strengthen how they identify and respond to safeguarding concerns where online activity may be contributing to harm.

This learning resource can be used by practitioners and leaders in supervision, team discussions and learning events to reflect on relevant safeguarding incidents relating to online harms and the multi-agency practice response.

Why is it important for children and young people?

Online interactions, including those that are abusive, coercive or exploitative, can reach into spaces previously considered safe, including the family home. Abuse, coercion and peer conflict may continue at any time, beyond school or community settings. As a result, children involved in serious incidents considered by the Panel may feel that they have no safe space: at home, at school, in their community or online.

> *"All staff need to be mindful that a family has had their world turned upside down, they are frightened for their child and of a suspect out there somewhere who was prepared to do harm and exploit."*
>
> Parent of a child who experienced online harms

This resource seeks to help multi-agency practitioners navigate a complex and growing area of safeguarding risk to children and young people. We recognise that there is a lack of visibility of online material viewed by children to parents and practitioners, as well as a lack of current regulation regarding the content that is accessible to young people.

The Government's recent announcement on a planned social media ban for under-16s on major platforms reflects wider concern about these risks. However, safeguarding learning highlights that harm continues to occur across a range of online environments, including those not captured by mainstream platforms.

What is the evidence base?

The Child Safeguarding Practice Review Panel's Annual Report (2024 to 2025) highlighted the occurrence of online harms in safeguarding incidents as an emerging trend with 9% (24) of all rapid reviews (274) received by the Panel during this time period reporting an online context to the harm caused to the child.

Online contexts, both directly relating to an incident and within a child's wider life, increasingly feature in the safeguarding reviews considered by the Panel. References to online harms in reviews have increased from 5% in 2022-23, to 7% in 2023-24 and 9% in 2024-25.

Of the twenty-four rapid reviews in 2024-25 that noted an online context:

- Fifty-eight percent (n=14) involved incidents of serious harm, particularly extra and intrafamilial child sexual abuse.
- Twenty-nine percent (n=7) were fatal incidents, with 4 of these identifying suicide as the likely cause of death.

- Thirteen percent (n=3) were for “other” incidents.

Learning from the Panel’s national and thematic reviews consistently shows that online environments feature in the experiences of children who have suffered serious harm, particularly in relation to:

- Child criminal exploitation (CCE) – where online platforms are commonly used for grooming, recruitment, coercion, and control, enabling perpetrators to initiate relationships rapidly and operate across local authority boundaries.
- Child sexual abuse (CSA) – where online spaces frequently function as sites of grooming, sexualised communication, and image sharing, sometimes preceding, replacing or coexisting with offline abuse.
- Neglect – where unmet emotional needs, limited supervision and weak protective relationships increase children’s vulnerability to online grooming, harmful content, and exploitation.
- Suicide – where children’s online relationships and interactions can lead to manipulation, coercion or exposure to harmful content, increasing the risk of suicide.

These issues are interconnected. Online activity may form part of a wider pattern of vulnerability and harm, including serious youth violence, and should not be considered in isolation from children’s wider experiences and relationships.

There are important limitations to this evidence. The Panel’s learning is based on cases notified through serious incident notifications and safeguarding reviews and therefore represents only a partial picture of safeguarding risk. Wider evidence points to emerging online threats that may not yet be fully reflected in referrals to the Panel, including risks associated with violent or fixated individuals and ‘Com’ networks. The National Crime Agency has highlighted the emerging threat posed by these networks and the risks they present to children and young people: National Crime Agency: Com groups early threat identification notice

There is a recognised disconnect between what is known to be occurring in children’s online lives and what is currently formally captured through safeguarding systems. Online harm is likely to be significantly under-represented in the cases received by the Panel.

In many cases, online harm may not be identified, explored, or recorded, even where it is a contributing factor to serious harm. This reflects challenges in professional confidence, identification and reporting.

As a result, the Panel’s findings should be understood as representing the currently visible aspect of a much wider and more complex safeguarding issue.

Key facts and figures

Between 1 April 2024 and 31 March 2025, the Panel received 274 rapid reviews.

Of these, 24, or 9%, specifically featured online harms.

Further data (unpublished) from 1 April 2025 to 31 December 2025 highlights that from 216 rapid reviews seen by the Panel over this period, 29 (13%) reported online harms. This illustrates that the prevalence of online harms in safeguarding incidents continues to rise.

These figures should be understood within the wider context set out above, recognising that they are likely to under-represent the true scale of online harm within safeguarding practice.

The following analysis focuses on the subset of rapid reviews in which online harms featured alongside risks outside the family home. Analysis of harm within the family environment is outside the scope of this section.

Risks outside the family home

1 April 2024 – 31 March 2025

Of the 24 rapid reviews which included online harms as a risk factor, fifteen of these also identified risks outside the family as a persistent theme. Five of these identified particular risks and concerns relating to online harms or activity including:

- concerns about the child sharing indecent images of themselves with adults online
- concerns about the child engaging with harmful online content relating to self-harm and harm of others
- concerns about the child in focus distributing indecent images of children
- concerns about social media use which put the child in focus at risk, with the serious incident itself videoed and posted online
- concerns about the child's use of social media

1 April 2025 – 31 December 2025 (unpublished data)

Of the twenty-nine rapid reviews which included online harms as a risk factor, twenty of these also identified risks outside the family as a persistent theme. Eight of these identified particular risks and concerns relating to online harms or activity including:

- concerns about the child's online activity which indicated potential exploitation or radicalisation
- concerns about the child's online activity which included CSE
- concerns about the child reporting they were in an online relationship with an adult in another country
- concerns about the child sharing indecent images of themselves with adults online
- concerns about the child receiving explicit images from adults online
- concerns about the child engaging in, and experiencing, online harassment and bullying
- concerns about the child sharing details of their experience of CSA on social media which placed them at further risk of CSA and CSE
- concerns about the child's underage social media use which placed them at risk of CCE and CSE

Across these cases, online harm frequently involves individuals, networks or influences **outside the family**, even where the activity itself takes place within the home. This creates a safeguarding context where harm is not confined to one setting, but spans home, peer groups and wider online environments.

This reinforces the Panel's position that harm outside the family, including peer and community-based risks, is increasingly experienced through online environments and cannot be clearly separated from them. Online content and interactions can lead to children feeling unsafe or threatened in the community and may prompt them to carry weapons for perceived self-protection, leading to an increased risk of physical harm. In many cases, this harm is difficult for parents and practitioners to observe directly, particularly where children are engaging in online relationships, accessing harmful content or interacting within networks that are not visible through traditional safeguarding routes.

This may include activity within closed or encrypted online networks, where risk is not easily visible and identification may rely on information being shared across agencies or through intelligence-led activity.

While there are clear limits to what parents and professionals can see of children and young people's online interactions, there is also a question about visibility within peer networks. In a number of cases that the Panel has seen, concerning online relationships are not identified by adults until after a serious incident, yet friends and peers may have been aware of them for some time because they share the same online spaces and see discussions unfold in real time. This suggests that the challenge is not always one of complete invisibility, but of recognising and acting on information that may initially appear as gossip or rumour.

There is likely to be existing good practice and ongoing learning for schools and other safeguarding agencies in this area. A key challenge is understanding where the threshold lies between informal peer information and indicators of potential harm, and how professionals can create environments in which young people feel able and confident to share concerns before risks escalate.

Common issues

Analysis of safeguarding reviews in which harm outside the family home featured alongside online activity identified the following common issues:

Online indicators of exploitation not recognised early. Concerning behaviours (e.g. contact with unknown adults, sexualised communication, online relationships) were often seen in isolation and not consistently identified as indicators of exploitation or grooming.

Failure to respond effectively to online relationships with adults (including overseas). Online relationships were sometimes underestimated in seriousness, with insufficient exploration of coercion, control, and risk.

Missed opportunities to investigate image-based abuse. Limited use of device checks, digital evidence and police investigations led to missed opportunities to identify perpetrators and disrupt harm to the child.

Children's online experiences not fully explored. Practitioners did not consistently demonstrate professional curiosity about children's online accounts and did not revisit this when concerns persisted.

Fragmented multi-agency response to online harm. Information about online risks (e.g. harassment, image sharing, grooming) was not always effectively shared or escalated, limiting coordinated safeguarding action.

Online harm not considered within wider vulnerability and cumulative risk. Risks such as bullying, sharing abuse experiences online and underage platform use were not consistently linked to exploitation, mental health risk, or wider harm outside the home.

Over-reliance on child or parent engagement. Lack of disclosure or engagement by the child (or parental oversight) led to reduced professional action, rather than proactive safeguarding responses.

Across these cases, a consistent theme is that opportunities to identify online harm were missed because practitioners did not routinely or confidently explore children's online lives. This reinforces that the primary challenge in many cases is not only responding to harm but recognising and understanding it at an early stage.

Hallmarks of good practice

Relevant cases seen by Panel highlighted the following examples of good practice:

Early recognition of online harm and exploitation. Practitioners identified online behaviours (e.g. sexualised communication, contact with unknown adults, or risky relationships) as potential exploitation or grooming at an early stage, rather than minimising or normalising them.

Timely and coordinated multi-agency response. Concerns about online activity (including CSE, image sharing, or online relationships) triggered prompt information sharing, strategy discussions, and joint safeguarding action, with clear roles across agencies.

Strong professional curiosity and analysis. Practitioners explored beyond initial disclosures, challenged inconsistencies and triangulated information across agencies, thereby ensuring a full understanding of risk and lived experience.

Child-centred and trauma-informed engagement. Children were supported to talk about online experiences in safe, trusted environments, recognised as victims of exploitation, not responsible for harm and provided with emotional and therapeutic support where needed. It is important that children are not made to feel guilt, shame or fear or have concerns about getting into trouble as this would hinder them from sharing their experiences.

Effective response to image-based abuse and digital evidence. Practitioners ensured appropriate police involvement, consideration of device examination and digital evidence and disruption of perpetrators where possible.

Holistic assessment of contextual and cumulative risk. Online harm is understood alongside bullying, poor mental health and poor emotional wellbeing, wider vulnerabilities (e.g. neglect, missing episodes) ensuring cumulative harm and harm outside the home are fully considered.

Clear focus on online safety and parental support. Work with families included exploring online platform use, underage access, and hidden accounts. Parents and carers were supported to understand and manage online risks.

Appropriate escalation and persistence. Practitioners escalated concerns even when children disengaged or minimised harm. Practitioners recognised that not hearing directly from a child does not reduce risk and ensured that safeguarding action continued.

These examples demonstrate that effective practice in an online context requires practitioners to take **active and specific steps** to understand children's digital lives, rather than relying on general approaches to safeguarding or waiting for disclosure.

Reflective questions for practitioners

Recognising exploitation in online activity

- When a child presents with concerning online activity (e.g. contact with unknown adults, secrecy, multiple platforms), do I actively consider risks of exploitation, coercion, or grooming, even where the child does not identify themselves as a victim?
- Am I analysing patterns over time (e.g. repeated incidents, missing episodes, prior concerns) to understand cumulative risk and harm, rather than viewing each episode in isolation?

Social media use and wider contextual risk

- Where appropriate, do I routinely explore the platforms a child is using, including underage access, and whether there are hidden accounts, multiple devices, or unsupervised use? Do I have the technical understanding to ask these questions and explore these issues confidently? If not, what training might I need to do this better?
- Do I understand any changes in a child's online activity and behaviours, such as newly downloaded apps or new accounts created on social media platforms, including those considered less 'mainstream'?
- Am I recognising that underage social media use can expose children to CCE or CSE, radicalisation, or involvement in harmful networks, and am I responding with appropriate safety planning and escalation?

Identifying and responding to CSE in online contexts

- Where children are engaging in sexualised online interactions, do I recognise these as potential indicators of CSE rather than consensual or experimental behaviour?

Online relationships

- When a child reports being in an online relationship with an adult or another child, including someone based overseas, do I explore issues of coercion, control, and grooming?
- Am I escalating and sharing information appropriately, even where the child withdraws or minimises concerns?

Online harassment, bullying, and peer harm

- When children experience or engage in online bullying or harassment, do I assess the emotional / psychological impact, including links to self-harm or vulnerability?
- Am I working with schools and partners to build a full picture of online peer dynamics and risk?

Reflective questions for leaders

Leadership oversight of online risk and exploitation

- Do we have an accurate and up-to-date understanding of online harm across our locality, including CSE, criminal exploitation, online grooming, and radicalisation risks? Are we also considering community-safety and place-based intelligence?
- Are we confident that patterns of online abuse (including image sharing, grooming, and coercion) are being recognised and escalated appropriately across services?

Contextual safeguarding and harm outside the home

- Are we confident that risks outside the home (including online environments) are central to safeguarding assessment and planning?
- Do we avoid over-reliance on parental protective capacity in situations where harm is occurring online, facilitated by peers or people unknown to the child?

Understanding and responding to online relationships

- Do we promote a culture where online relationships are understood as real and emotionally significant, rather than less serious than offline relationships?

Online image sharing and sexualised behaviour

- Are we confident that practitioners recognise risks where children are sharing indecent images of themselves as well as understanding that this may be linked to grooming, coercion, or exploitation (including the use of AI generated sexual images)?

Multi-agency working and information sharing

- Do all agencies share a consistent understanding of online harm, including indicators, thresholds and required responses and are all key agencies involved early and consistently in cases involving online harm?

Professional curiosity, skills, and training

- Are leaders confident that practitioners have the confidence and competence to discuss online activity as well as an up to date understanding of platforms, trends, and risks? Do practitioners and leaders know how to act against inappropriate content discovered online, including how to report content to platforms for removal? When did we last review our training offer for online harms?
- Is there a culture of professional curiosity, where practitioners actively explore online activity and do not rely solely on child disclosure?

Case study

The following example from a safeguarding review highlights how serious harm can occur through online relationships that are invisible to practitioners and families.

A 13-year-old girl appeared engaged with school, therapy and family support but was experiencing underlying emotional vulnerability connected to her early life experiences and identity. This included an earlier incident where the child had been in contact with an individual online who had misrepresented their identity ("catfishing").

In the weeks prior to her death, she formed an online relationship with a young adult male in another country. This was unknown to all practitioners involved in her care. It is suspected that she was groomed through this online contact and influenced into taking her own life.

Learning points

Serious harm can occur in unseen digital spaces, and safeguarding practice must routinely include active exploration of children's online lives, relationships, and behaviours, supported by strong multi-agency communication and professional confidence in addressing online risk.

- Online harm must be proactively explored. Practitioners did not ask about or understand the child's online life even though there was evidence of an earlier "catfishing" incident.
- Greater professional curiosity was required. Practitioners relied on the child to talk about concerns rather than actively exploring potential risks, particularly in digital spaces.
- Children's emotional vulnerabilities increased online risk. The child's attachment needs and "connection-seeking" behaviour increased her susceptibility to grooming and this was not sufficiently explored.
- Practitioners needed better awareness and confidence around online safety. Many practitioners lacked familiarity with online platforms and risks.
- Improved multi-agency communication and coordination was needed. Services (e.g. therapy providers, GP, school) were not fully aware of each other's involvement. This reduced opportunities for holistic understanding and risk identification.
- Hidden risk may not be identified through standard assessments. The child appeared positive, engaged, and future-focused and existing assessments did not capture the unseen risk occurring online.

OFFICIAL - FOR PUBLIC RELEASE

- Recognise the benefits of online activity while actively exploring risk. While the online world offers many benefits, practitioners should remain curious and ask specific questions, recognising that serious harm may remain unseen unless children's online relationships and experiences are actively explored.

Where can I find out more?

Find more information and resources on the Child Safeguarding Practice Review Panel Learning Hub.

Other useful resources include:

- Child Safeguarding Practice Review Panel: Annual Report 2024 to 2025
- Growing up in the online world: a national consultation
- National analysis of police-recorded child sexual abuse and exploitation crimes: 2024
- The Southport Inquiry: Phase 1 report
- Southport Inquiry: Phase 2 terms of reference
- NSPCC: Online abuse and bullying prevention guide
- Local Government Association: Online harms
- UK Safer Internet Centre
- NCA-CEOP: Guidance, policy and research for professionals
- Youth Justice Resource Hub: Online harms affecting children evidence pack
- Online Safety Act: explainer
- 'What I wish my parents or carers knew…': A guide for parents and carers on managing children's digital lives | Children's Commissioner for England]