MODERN SLAVERY & HUMAN RIGHTS | POLICY & EVIDENCE CENTRE

Led by the University of Oxford

Understanding the Online Recruitment of Children into Criminal Exploitation in the UK

Research Report

November 2026

Author: Dr Anna Skeels (SPARK, Cardiff University)



Research by

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

Social Science Research Park
Y Parc Ymchwil Gwyddorau Cymdeithasol

'...there is good reason to believe that some forms of child exploitation operate outside current understanding, that children and young people are being victimised every day in ways that are not recognised.' [1]

[1] The Children's Society (2025a:4)

Authors

This is the final research report on Online Recruitment of Children into Criminal Exploitation in the UK, based on research conducted by Dr Anna Skeels, Research Fellow from SPARK, Cardiff University, with Hannah Stott from Safe to Grow in partnership with Barnardo's Independent Child Trafficking Guardianship (ICTG) service.

Acknowledgements

The authors gratefully acknowledge the support from Barnardo's Independent Child Trafficking Guardianship (ICTG) service for this research, as well as the participation in interview of practitioners working with children affected by Child Criminal Exploitation in the UK and the lived experience expertise shared by the PEC LEAP. This research would not have been possible without them.

Content Warning

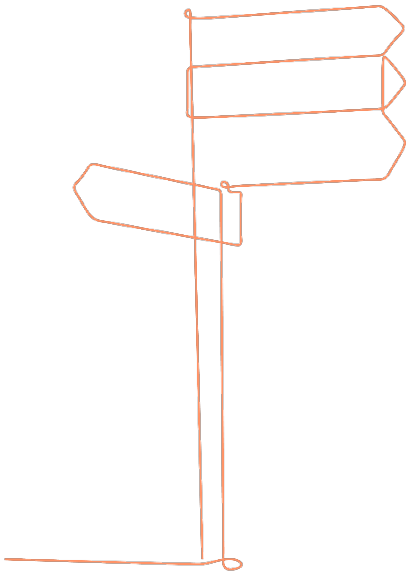
This research, while not engaging children directly, is concerned with how children are being recruited online into criminal exploitation in the UK. The report includes accounts from practitioners working with those children affected, describing the situations children are being recruited into, the ways they are being groomed and coerced into criminal activity and the harms experienced.

Funding

This research is funded and supported by the Modern Slavery and Human Rights Policy and Evidence Centre (PEC), University of Oxford, which in turn is funded and actively supported by the UK Arts and Humanities Research Council (AHRC). The views expressed in this report are those of the authors and not necessarily those of the Modern Slavery and Human Rights Policy and Evidence Centre, the University of Oxford, or the Arts and Humanities Research Council.

Abbreviations

CCE Child Criminal Exploitation
CSE Child Sexual Exploitation
IASC Independent Anti-Slavery Commissioner
ICTG Independent Child Trafficking Guardian
LEAP Lived Experience Advisory Panel
NEET Not in Education, Employment or Training
NRM National Referral Mechanism
OSA Online Safety Act
PEC Modern Slavery and Human Rights Policy and Evidence Centre



Contents

1: Headline Findings and Recommendations 5
2: Introduction and Background 7
2.1 Child Criminal Exploitation and Children's Digital Lives 8
3: Methods and Approach 10
4: Findings: Context 12
4.1 A Gap in the Evidence 12
4.2 Online Recruitment at Scale 14
4.3 Digital Platforms 15
4.4 Children at Risk 19
5: Findings: Mechanisms 26
5.1 Recruitment Process and Tactics 26
5.2 Recruitment Pathways 27
6: Findings: Outcomes 44
6.1 Harms to Children 44
6.2 Mitigations and Interventions 46
7: Conclusions 55
8: Recommendations 57
9: References 59

1: Headline Findings and Recommendations

Headline Findings

Children affected by online recruitment into criminal exploitation in the UK remain relatively unseen and require our urgent attention.

- **Key Finding 1:** Children are being recruited into criminal exploitation online at scale across multiple digital platforms, placing a far broader group of children at risk and resulting in widespread, significant harm.

- **Key Finding 2:** Online recruitment pathways and tactics vary, intersect and continually evolve, making them difficult to identify and mitigate against. As a result, many cases are unrecognised and under-investigated.

- **Key Finding 3:** Ten online recruitment pathways into Child Criminal Exploitation (CCE), associated risk factors and outcomes, are identified through this research. They demonstrate the intersectionality of CCE and Child Sexual Exploitation (CSE) and how online and 'offline' tactics and harms interconnect. Other pathways can and do exist. No digital platform should be overlooked in relation to recruitment.

- **Key Finding 4:** Mitigation of online recruitment into CCE is inadequate. Practitioners are under-equipped and overwhelmed in their efforts to prevent and disrupt harm. A lack of data, research and children's participation are an obstacle to addressing the problem and to co-designing effective interventions.

- **Key Finding 5:** A system-wide, coordinated response to the online recruitment of children into criminal exploitation is required, building on existing relevant efforts, for example, those effectively preventing online grooming into CSE and addressing child exploitation 'offline'.

Recommendations

The following should be read and considered in conjunction with the broader, system-level recommendations addressing the exploitation of children in the accompanying Gap Analysis report.

- **Recommendation 1:** The UK government should make CCE a priority offence under the Online Safety Act (OSA) by including it in Schedule 7 of the Act. This new CCE priority offence should not be siloed but considered alongside other

priority offences, existing and future, relating to child exploitation and human trafficking as well as harmonised with the 2026 Crime and Policing Act definition of CCE. Statutory guidance on CSEA harms should explicitly recognize how child sexual exploitation (CSE) and intimate image abuse can be criminally motivated and intersect with CCE.

- **Recommendation 2:** Ofcom should address CCE in the Children's Code of Practice and include it in the Children's Register of Risks as an additional risk. The new entry in the Children's Register of Risks should recognize the interconnection of CCE with multiple other risks, harms and offences that 'victims' of CCE can encounter, such as, but not limited to, grooming, intimate image abuse, and coercive and controlling behaviour.[1] CCE should also be recognized in Ofcom's general online safety Register of Risk.

- **Recommendation 3:** The forthcoming MoJ Statutory Guidance on the Crime and Policing Act 2026 must recognize online recruitment into Child Criminal Exploitation (CCE) and CCE as manifest online in its formal definition of CCE. The Guidance should raise awareness of the potential risks to children of being recruited online into criminal exploitation, the methods employed by perpetrators and the harms involved. The interconnection between online and 'offline' tactics and harms as well as between CCE and CSE and other forms of child exploitation and human trafficking must be highlighted.

- **Recommendation 4:** The IASC working with the Department of Education, Home Office and devolved equivalents should raise awareness of all 'first responders', guardians and trusted adults on - and drive integration of - the online recruitment of children into criminal exploitation into multi-agency, child-centred efforts to safeguard children from exploitation. Such collaborations should include the ongoing identification of gaps in knowledge and safeguarding practices related to online recruitment, as well as the development of tools, resources and mechanisms needed by frontline practitioners for support.

2: Introduction and Background

This report investigates the online recruitment of children[2] into criminal exploitation in the UK. It is based on a six-month research project commissioned by the Modern Slavery and Human Rights Policy and Evidence Centre (PEC) at the University of Oxford, funded by the Arts and Humanities Research Council (AHRC). The main research question is:

How does the recruitment of children in the UK into criminal exploitation manifest online, and how can digital environments mitigate against this?

Child Criminal Exploitation (CCE) is child abuse, a serious violation of children's rights and a criminal offence under the Crime and Policing Act 2026. Protection against prosecution for offences committed due to their exploitation is provided for 'victims'[3] of CCE under the UK Modern Slavery Act 2015.[4]

Recruitment of children in the UK into criminal exploitation is happening increasingly online, but the extent and nature of such online recruitment have remained poorly understood. This report responds to the gap by exploring the digital platforms and recruitment pathways involved, the children who are most at risk, the tactics and mechanisms employed and the resulting harms. The report is based on three interconnecting sources of evidence: review of academic and 'grey' literature, semi-structured interviews with practitioners working on CCE and engagement with the Lived Experience Advisory Panel (LEAP) of the Modern Slavery and Human Rights PEC.

This Main Report is accompanied by a separate but interconnected report on legal and policy frameworks and online recruitment into CCE. This accompanying report identifies the gaps both within and in-between these frameworks where this problem might be better addressed. It should be read in conjunction with this report.[5]

Recommendations for policy, practice and future research are set out separately in these two reports and then combined in our Research Summary.

2.1 Child Criminal Exploitation and Children's Digital Lives

Child Criminal Exploitation (CCE) is defined by The Children's Society as:

'...a form of child abuse in which a young person is manipulated or pressured to take part in criminal activity, often through threats of violence alongside serious physical, emotional and sexual harm' (**The Children's Society, 2024:9**)

Criminal exploitation, including of children, has received growing attention in UK policy and practice over the past ten years. The Centre for Social Justice (2024) notes that this was the most prevalent form of 'modern slavery' in the UK between 2020-24, involving primarily the exploitation of British nationals, mostly teenagers, into committing crime for someone else's benefit.

In the UK in 2025, 30% (7028) of a total of 23,411 potential 'victims' of 'modern slavery' referred via the National Referral Mechanism (NRM)[6] were children under the age of 18 (UK Government, 2026). These children were mostly referred for CCE (50%; 3,485). Male children also accounted for 76% (1,585) of the 2,083 'county lines' flagged referrals for that year. Due to its hidden and under-reported nature, however, the actual prevalence of CCE is considered far greater.

Home Office Guidance on 'county lines' (UK Government, 2023) focuses on exploitation related to the supply of drugs and transportation of associated money and weapons. Criminal exploitation is not limited to 'county lines', however, and can include, for example, coercion into burglary, theft, pickpocketing, shoplifting, violent offences (Centre for Social Justice, 2024), financial crimes (The Children's Society, 2025a and 2025b) and cannabis cultivation (Dixon, 2023).

This increased focus on CCE has informed a relatively new approach to child protection, known as 'contextual safeguarding', concerned with harm outside the home. Digital platforms are one domain where such extra-familial harms can occur (Firmin, 2020:4).

The internet and digital technologies have transformed children's lives. Children can be the first to use new technologies, often becoming the 'teachers of their parents and carers' in this regard (Palmer, 2015:13). Children's device ownership and online activity have risen sharply, and ever-younger children are going online, a trend accelerated by the Covid-19 pandemic and lockdown and which has continued. Palmer states that 78% of 12-15-year-olds own a mobile phone (65% of these a smartphone) and 31% (20%) of 8-11-year-olds respectively (2015:6). Drawing on Ofcom statistics, The Children's Society (2024) notes that while many

social media platforms' age limits are 13+, 60% of 8-12-year-olds said they had set up their own social media accounts.

Children's digital engagement has reshaped their experiences and relationships. Children often refer to their online contacts as 'friends', even if they have never met them face to face. Children's online and 'offline' worlds have become interconnected so that **'to a young person who has grown up in the digital age, what happens in the online world is as real as what happens offline'** (Barnardo's, 2023a:2). This shift is essential context for this research.

Although the internet offers learning and developmental benefits for children, it has expanded opportunities for their exploitation. Larasati and Wahyudi (2021) argue that it has widened criminals' reach and enabled manipulation through platforms without strict age verification. Scanlan et al. (2022) note the relative anonymity and low detection risk for the perpetrators of such 'digital crimes', and Palmer (2015) emphasises the accessibility and availability of children to perpetrators online.

The Children's Society defines **online** child exploitation as: **'...an individual or group using online platforms to take advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual and/or criminal activity that can occur both online and offline'** (2025b:5)

This recognition that child sexual and child criminal exploitation can overlap and that exploitation can move between digital and 'real life' domains, reflects the 'hidden harms' and 'complex and interconnected threats' faced by children both online and offline (Barnardo's, 2023a:2). Importantly, Barnardo's states: **'Now, online harm is present in almost all cases of child sexual and criminal exploitation'**(2023b:5).

[1] This research demonstrates the interconnections between the online recruitment of children into criminal exploitation and other risks, harms and offences already included in the Children's Register of Risks including CSEA, terrorism, grooming, hate, intimate image abuse, harassment, stalking, threats and abuse offences, coercive and controlling behaviour, fraud and financial offences, proceeds of crime, drugs and psychoactive substances, human trafficking and firearms, knives and other weapons.
[2] 'Children' are defined for the purposes of this report, as under the UN Convention on the Rights of the Child (UNCRC), as any person under the age of 18.
[3] Children affected by child criminal exploitation are commonly referred to as 'survivors' of exploitation to counter criminalisation and victim blaming. However, in law, for example the UK Modern Slavery Act 2015, the term 'victim' is used.
[4] Child criminal exploitation is not explicitly listed as an offence under the UK Modern Slavery Act 2015. However, the Act provides a statutory defence (Section 45 of the Act) for victims of child trafficking and modern slavery accused of criminal offences, including relating to child criminal exploitation.
[5] Stott, Hannah. Forthcoming 2026. Understanding Online Recruitment of Children into Criminal Exploitation in the United Kingdom: Gap Analysis.
[6] The National Referral Mechanism (NRM) is the framework established by the UK Government for identifying and supporting individuals who may be victims of modern slavery and human trafficking.

3: Methods and Approach

The report uses three different interconnected methods to understand online recruitment into CCE:

(1) a review of academic and 'grey' literature;
(2) semi-structured interviews with practitioners working on CCE; and
(3) online engagement with the PEC Lived Experience Advisory Panel.

These three methods are combined in a 'realist-informed review', drawing from a relatively new approach synthesising findings from pre-existing literature with direct engagement of stakeholders as participants in the research. Combining previous published evidence with practitioners' views and the lived experiences of people affected by exploitation provides a more comprehensive and reliable picture than literature review alone, crucial for understanding a complex and emerging issue which has been under-researched to date.

A 'realist review' aims to identify **'what works for whom, in what circumstances, in what respects and how'** (Pawson et al, 2005: 21), examining interactions between **'context'**, **'mechanism'** and **'outcome.'** Expert (including lived) experiences and perspectives are therefore key. Realist reviews are also used to explore and diagnose 'the underlying causes of problems' (Duddy and Wong, 2023: 175). With a focus on the 'problem' of recruitment into CCE online and how recruitment pathways operate across digital contexts with resultant harms for children, this approach is appropriate for this research. Realist reviews, however, can involve 'considerable and sustained investment over time' with a 12-24-month turnaround required. Given this project's six-month duration and current policy relevance, a **'*rapid* realist review'** was employed, suiting 'the time-sensitive demands of many policy decisions' (Saul et al, 2013:2).

'Rapid realist reviews' engage stakeholders as a 'reference panel' and 'expert group' to help make sense of and build on the literature. Identification of documents for inclusion in the review (both academic and professional literature) often begins with those identified by such stakeholders and experts. In addition, relevant search terms are used to iteratively generate lists of documents that may be included in the review. 21 NGO reports were identified by Third Sector partners The Children's Society, NSPCC and Barnardo's as relevant to the review. Searches were conducted via Google Scholar, ProQuest Social Science and Scopus using multiple appropriate search strings. No academic publications were identified since 2021 with 'online child criminal exploitation' as an exact phrase or with all these words in the title and less than 20 publications on each platform with 'child criminal exploitation' in the title. Once search terms were wider, for example 'online exploitation' and 'children'

or 'grooming children online', hundreds more publications resulted, many related to CSE.

Because of the very limited academic research on the online recruitment of children into CCE identified via the literature review, the semi-structured interviews with cutting-edge practitioners working in this field and direct engagement with the lived experiences of the PEC's Lived Experience Advisory Panel (LEAP) were crucial, current sources of evidence for this research. Online interviews were undertaken with 12 expert practitioners working with children affected by CCE in the UK. In these interviews, practitioners drew on their work, caseloads and tacit knowledge to describe the digital platforms, design features and online communities being used for recruitment, the risk factors associated with children most affected, the strategies and grooming tactics exploiters employed, the intersecting harms for children and suggestions for mitigation and change. What came across was a strong and aligned sense of what they are seeing, hearing, reading, responding to, struggling with and addressing in their practice to tackle online recruitment into CCE. In keeping with a 'realist' approach, interview data was thematically analysed and coded against a **'context'** (digital platforms and design; risk factors to children) **'mechanism'** (pathways and tactics) and **'outcome'** (harms) framework with further sub-codes arising out of the data and mitigations/interventions as an additional code. However, while the research follows this broad realist approach - identifying contexts, risk factors, mechanisms and harms - insufficient data was available for a more detailed disaggregation of outcomes by groups of children required for a full 'realist review'.

Two interactive online sessions were also held with the PEC's Lived Experience Advisory Panel LEAP. This is essential for acknowledging and respecting the centrality of survivor voices and lived experiences for any research on exploitation as well as for the unique form of evidence and critical perspectives that only such contributions can bring. Both sessions broadened our understanding of the issue, generated new insights and helped us to gain 'thicker' descriptive data, given the limited relevant academic sources identified via the review. Session 1 with the LEAP (25 February 2026) involved sharing key messages and recruitment pathways emerging from initial literature review and ideas for solutions. Feedback from this session has fed mainly into this report. Session 2 with the LEAP (20 May 2026) involved validation of our summary from the previous session and discussing draft ideas and priorities for research impact on policy, practice and law. This discussion has more broadly informed our recommendations.

Children affected by online recruitment into criminal exploitation did not participate in the research. This was agreed by all partners involved, due to the limited timeline, considered insufficient for children's safe and meaningful engagement. **All children have the right to participate in matters and decisions affecting them under Article 12 of the United Nations Convention on the Rights of the Child. The experiences, views and perspectives of children affected by online recruitment**

into criminal exploitation are essential for us to fully understand and address this problem.

This research also looks beyond the role of digital environments to the wider legal and policy landscape and explores to what extent the online recruitment of children into criminal exploitation is addressed by relevant UK legal and policy frameworks and what gaps exist. A targeted, desk-based **gap analysis** was employed as a systematic approach. This method can be useful to tackle complex social problems where legislation and policies play a crucial role in guiding decision-making, multi-agency collaboration and best practice.

4: Findings: Context

4.1 A Gap in the Evidence

Based on our review, academic literature on CCE in the UK includes relatively little on how this manifests online. No academic publications were identified through the review with 'online child criminal exploitation' (or equivalent terms) in their title or as their substantive focus. Of those authors writing significantly, expertly and in detail about CCE in the UK, references to CCE's digital dimension are patchy.

For example, academic publications on CCE in Wales - including Maxwell et al (2019), Maxwell and Wallace (2021), Maxwell (2023), Maxwell and Corliss (2024), Maxwell (2026) – often directly engaging young people affected by CCE and/or their parents, refer briefly to 'social media' or 'online' less than 10 times combined. While very brief, these instances include mention of: 'social media' being used to control, shame and coerce criminally exploited boys (2019:30); 'online' environments as spaces of extra-familial harm and exploiters contacting children who have been relocated by/with their parents via gaming channels and their mobile phones (Maxwell and Wallace, 2021:14 and 45); parents struggling to limit the 'social media use' of adolescents at risk of CCE (Maxwell, 2023) and children being approached 'online' or in person by their peers in relation to CCE and being presented with images of 'extravagant lifestyles' and 'money' via 'social media' (Maxwell, 2026:55-66).

Studies relating to CCE in Northern Ireland - including Walsh (2023) and Kane and Chisholm (2025) - similarly briefly mention examples of how this manifests online. Walsh (2023) includes reference to 'social media' - and more specifically Facebook and Snapchat - including in quotes from research participants, in relation to grooming and access to drugs. No reference is made to 'online' contexts where **'contextual safeguarding'** is outlined. Walsh also notes the mechanisms around which CCE is uniquely operationalised in Northern Ireland and includes the 'threat of

exclusion' from the 'entire community' including 'online platforms' and 'social media', having more hold over young people being exploited through CCE than the 'very real' threat of the violence (2023:299). Kane and Chisholm mention only that CCE 'can occur through the use of technology and social media' (2025:11) and that the definition of human trafficking from the Palermo Protocol is 'broad enough' to encompass 'online exploitation' (2025:23).[1]

Studies exploring CCE in England include, for example, Robinson, McLean and Densley (2019) and Robinson (2020) on Merseyside, the latter with a brief mention of the impact of 'technology' on county lines, gangs and CCE and the former noting that 'CCE does not necessarily involve physical contact' and can occur online, on social media and on smart phones (2019: 697). There is also a mention of how 'gang members…display the glamorous aspects of their lifestyle' both in person and on social media (2019:707).

Dixon's (2023) study of CCE in Scotland, engaging residential care workers and other professionals and drawing on a range of sources, provides more information on online CCE, including a dedicated section on 'social media and technology'. The coverage of this issue is broad but not in depth. Dixon is clear that 'victims of CCE can be targeted face-to-face or through social media' (2023:35), recognises the role of the COVID pandemic in children's increased engagement and exploitation online, mentions multiple digital platforms being used for recruitment (Snapchat, Instagram, WhatsApp, Telegram, Wickr, YouTube and online gaming platforms), albeit in brief, the role of social media in the glamourisation of criminal activity and digital methods used by exploiters for surveillance and control. What is missing, however, is the detail of recruitment pathways and the related risks and harms for children, a gap this report aims to address.

Prominent conceptual works relating to CCE are Firmin's publications on 'contextual safeguarding'.[2] In her 2017 publication, Firmin includes both physical settings (peer groups, schools and neighbourhoods) as well as broader social environments, including 'online social media', as contexts that shape peer-to-peer abuse. In Firmin (2020) she builds on this approach to understanding and responding to young people's experiences of significant harm beyond their families, with interventions focused on the contexts in which that harm occurs, including digital environments (Firmin et al 2022;2024). However, there is limited or no mention of the digital or online world or social media in many of the other publications listed below, nor any detail of how harm manifests in digital settings across this whole body of work. Other conceptual publications, for example Barlow et al.'s (2022) 'circles of analysis' systemic model of CCE significantly does not incorporate or mention the digital realm.

The academic literature indicates a strong imbalance between research on (recruitment into) online CCE and (grooming into) online CSE, with the latter represented by a much larger and well-developed body of UK and international evidence.

Other and more detailed evidence on the online recruitment of children into criminal exploitation can be found in the 'grey' literature in NGO reports. Third Sector child-centred organisations, including Barnardo's, the NSPCC, The Children's Society, Action for Children and others, have all been reporting on this issue for some time, predominantly post the COVID pandemic and UK response in 2020-21 and including in relation to the Online Safety Act. This includes in-depth reports on specific types of online child criminal exploitation, for example on the financial exploitation of children (The Children's Society, 2025a and 2025b) or on exploring digital platform risks for certain groups, for example women and girls (NSPCC, 2025).

These sources and others identified through the review are drawn upon where relevant for this report, alongside original primary data from our interviews and sessions with the LEAP.

4.2 Online Recruitment at Scale

Barnardo's reported a rapid increase in online child sexual and child criminal exploitation in recent years, for example with online grooming crimes rising by more than 80% between 2018 and 2022 (2023b:23). The Children's Society in 'Keeping Children Safe Online' (2026)[3] note that 4 in 5 parents are worried about their children being groomed online for criminal exploitation with 56% thinking the greatest risk comes from social media.

These findings from the literature were corroborated by our interviews with experts within the sector. Practitioners working on CCE in the UK and participating in our research were clear that recruitment of children online into criminal exploitation is happening, now, and at scale.

One interviewee commented that he'd seen **'a massive…increase in online exploitation leading to criminal exploitation'** in the 'last, probably, two years' and 'more so in the last three to four months' (Interviewee 8). While no data is being formally or systematically collected through the NRM on the numbers of children being groomed online into criminal exploitation, these practitioners reported that children are being recruited and harmed at pace and they cannot keep up:

'It's a massive shift…because we, as much as anybody else, struggle to keep up with the next…online grooming technique that they're using…you understand one and by the time we've done that, they're using something else…the speed at which these… perpetrators…utilise that online world…is far more advanced than professionals around the table can be in response…' (**Interviewee 9**)

There was clear consensus across all practitioners interviewed on the extent and urgency of children being recruited online into criminal exploitation. This sits in stark contrast with the mostly marginal attention given to this issue in academic research. This is clearly a significant gap that is not being academically explored.

This begs the question as to why this is the case and why this problem - and those children who are being recruited into CCE online - are less 'seen'.

The practitioners we interviewed held detailed and highly current knowledge of the problem and its impact on children and were calling out for support. Given the even more hidden nature of children being targeted and exploited online, they suspected the problem is far greater:

'...we don't actually know how many young people are affected by this...and so many young people slip through the net, especially with online...recruitment...How many young people are sitting in their bedrooms, and we just don't know that this is going on?' (**Interviewee 4**)

This is clearly an area that needs urgent and substantive attention.

4.3 Digital Platforms

'...it can happen absolutely anywhere...that's really important for us to remember' (**Interviewee 1**)

Multiple digital platforms (and platform types) were identified in connection with online recruitment of children into criminal exploitation through the research, set out in **Table 1** below. The LEAP (Session 1, 25 February 2026) also emphasised that recruitment occurs through multiple digital platforms, not just gaming sites. Practitioners interviewed were keen to emphasise that recruitment can happen on *any* digital platform but that perpetrators will focus on platforms that children use the most, for example Snapchat.

Table 1: Platforms identified through the research used for online recruitment into CCE

Digital Platform Type	Examples from Research	Literature Review	Interviews
Traditional Social Networking Platforms	Facebook	✓	✓
	LinkedIn		✓
	X (Twitter)		✓
Image-Based Social Media Platforms	Instagram	✓	✓
	Snapchat	✓	✓
	Tumblr		✓
Short-Form Video Platforms	TikTok	✓	✓
	YouTube	✓	✓
Digital Communication Platforms	WhatsApp	✓	✓
	Telegram	✓	✓
	Wickr	✓	
Digital Communities	Discord		✓
	Facebook	✓	

Gaming Platforms Games	Twitch	✓	
	Discord		✓
	Roblox	✓	✓
	PlayStation3		✓
	Xbox / Xbox Live	✓	✓
	Twitch	✓	✓
	Nintendo		✓
	Grand Theft Auto	✓	✓
	Fortnite	✓	✓
	Call of Duty	✓	✓
	Cunch Chronicles		✓
	Drug Deal		✓
	Simulator	✓	✓
	Valorant	✓	
	FIFA		✓
Apps / Other	Wizz		✓
	OnlyFans		✓
	Grindr	✓	
	Dark Web	✓	
	Fortune		✓
	Omegle		✓
	Tinder	✓	
	ooVoo	✓	
	MyLOL	✓	

In the context of CCE, Dixon considers **Snapchat** as 'one of the main apps being used to communicate with children': 'it is easy to add friends, there is no historical feed of information and images and videos can disappear after a period of time' (2023:36).

The Children's Society has identified Snapchat as a 'favourite among teens' and set out risks the platform poses to children. Concerns include age verification (the minimum age is 13 but, with limited checks, younger children are accessing the platform), exposure to harmful material (through the Discovery feature which collects content from a wider audience) and the quick connections that can be made through username searchers, Snap codes and even by location: **'...this ease of connection can increase the chances of children connecting with strangers...it also opens the door to more serious contact, such as grooming and sexual abuse.'**[4]

This concern was supported by interviewees engaging in our research, who described Snapchat as one of - if not *the* - primary digital platform being used to recruit children into criminal exploitation. Snapchat was also reported to have had a role in multiple stages of the grooming process:

'…your…main one, in my experience… will be… Snapchat. It's…top of the list in terms of…recruitment and…ongoing comms and… keeping tabs on exploited persons. It's almost a fit-for-purpose kind of app, really, in that sense. It's almost as though we've designed for it.' (**Interviewee 3**)

All except one (Interviewee 6) of the 12 practitioners interviewed for the research spoke about Snapchat and in total Snapchat was mentioned over 80 times. Snapchat features mentioned by respondents included end-to-end encryption, disappearing messages and Snapchat 'stories' (photos and videos which disappear after 24 hours), the latter 'the main one we see in our referrals' (Interviewee 8). They felt that these enabled recruitment pathways into criminal exploitation through moving contact between exploiters and children from initial more 'open', mass messaging into a more private and secure domain and/or providing more personal information on the child.

Snapchat was also mentioned as enabling in the later stages of exploitation, for example a perpetrator posing as a child, using his Snapchat account to message his mother 'to say that he was safe and he'd only be away the weekend' (Interviewee 4), thus avoiding police attention and any escalation for a missing child.

Instagram was also mentioned by all except one (Interviewee 3) of our 12 interviewees as a platform for recruitment, with a total of 48 mentions overall - 'Instagram is also used quite frequently' (Interviewee 2) – and often interchangeably with Snapchat:

'…a perpetrator that finds a young person in real life, they swap numbers…they add…each other on Snapchat, the perpetrator follows them on Instagram. Then that perpetrator has…24-hour access to that young person at that point…' (**Interviewee 1**)

One interviewee mentioned Instagram being used by exploiters to expose children to and normalise violence to recruit them (See Recruitment Pathway 7 below).

Anonymity, disappearing messages and end-to-end encryption, common to Snapchat and Instagram, were also flagged as enabling recruitment through digital communication platforms like WhatsApp and Telegram:

'WhatsApp and Telegram are particularly big ones and perpetrators…like to use these because they both have end-to-end encryption, which obviously makes it much harder for safeguarding professionals to then get access to the evidence of that grooming and exploitation.' (**Interviewee 1**)

WhatsApp was mentioned by six respondents (Interviewees 1, 5, 6, 9, 10 and 12), 24 times in total and Telegram by four respondents (Interviewees 1, 5, 7 and 8), 14 times in total. Interviewees were concerned about Telegram, because it was less well known and operated more 'under the radar' while WhatsApp (Interviewee 5), by contrast, is a far more popular application and so less commonly considered as a means for recruiting children into criminal activity:

'…mass messages…via WhatsApp! They didn't need access to any other social media platform… It was a messaging app…my son hasn't got a phone but one of…his friends did. And I remember her [mum] saying to me… 'Oh, I've taken all of those things off her phone now'. And I said, 'but it was via WhatsApp. You use WhatsApp to drop her a message and say, 'what are you doing after school?'!' (**Interviewee 5**)

This is pertinent given the recent UK Government's recent announcement of a social media ban in 2027 for under 16s, which does not include WhatsApp.

TikTok was mentioned by seven interviewees (2, 3, 4, 5, 7 and 12), a total of 18 times, mainly in relation to its accessibility (Interviewee 4), and glamourising and normalising criminal activity and related criminal 'lifestyle' including money, clothes, drugs and cars:

'TikTok…there is a lot of content that…romanticises the concept of children being in particularly unsafe situations, which…when they get approached by recruiters, it doesn't seem off. It's almost like a normalised thing or like a status thing for kids.'
(**Interviewee 2**)

All 12 respondents in our research referred to gaming platforms as a recruitment space for children into criminal exploitation, with a total of over 70 mentions across all interviews. Discord and Roblox were highlighted particularly as popular digital gaming platforms used by online gamer communities.

Six respondents (Interviewees 2, 5, 7, 8, 11, 12) mentioned recruitment into criminal exploitation via Discord, a total of 11 times and four (Interviewees 3, 8, 9, 10) mentioned Roblox, a total of 8 times:

'Gaming is also…such a big space and community. There's Discord that a lot of people use for gaming, for streaming content online, which is also another big space for recruiters.'
(**Interviewee 2**)

'Gaming Apps…Roblox…for example…that kind of thing and that…kind of comms, again, perfect scenario for…the recruitment of children…in terms of exploitation.'
(**Interviewee 3**)

Respondents felt that a greater focus on recruitment via these digital platforms was needed, including the potential for further regulation of online spaces. Interviewees cited a lack of rigorous age restrictions as one of the factors facilitating the online recruitment of children, while others stated that limited awareness of how these digital platforms operate contributes to cases of online child criminal exploitation being overlooked:

'I think gaming platforms is something we're not picking up on. I don't think police are investigating it very well…because it's something that's not really known…how children are being exploited on gaming platforms, but it is happening…' (**Interviewee 8**)

'And…that's a space that is not regulated as well, the shared platforms for video games or online streaming, there's not a lot of regulation because you don't know who's coming in and who's going to be a part of it, and there's no age restriction on it as well. So, you

could have a 40-something year-old person playing with a 12-year-old, a 13-year-old. And if they say the right words, if they say the right things, it's easy to use that bonding or that connection as a gateway into that individual and their group.' (**Interviewee 2**)

Some respondents spoke about specific games that could be downloaded as apps or played via Discord and how their focus and content connected to, normalised and glamourised 'county lines' activity, playing a role in the grooming process:

'There are games which…children can download on the App Store, for example, literally, a game called Drug Deal Simulator…that is, you know, so absolutely damaging to children because it…outlines a life where this is great, this is fun, this is what I could do!' (**Interviewee 3**)

'There was a game not so long called the Cunch Chronicles. It was a…little platform game, right and it was like a like a 'county lines' game. So, you picked up a package and then you had to deliver this package on the screen…So, if children played it, they [perpetrators] could message them in that' (**Interviewee 8**)

Recruitment via gaming platforms / communities is mentioned in more detail in Recruitment Pathway 3 below.

Finally, **Facebook**, **LinkedIn** and **X** (**Twitter**) were all mentioned in interviews for the research, with Facebook also mentioned through the literature review. 8 out of our 12 respondents mentioned Facebook (Interviewees 2, 3, 4, 6, 8, 9, 10, 12), a total of 27 times. LinkedIn was mentioned by one person (Interviewee 3) and Twitter by one person (Interviewee 2). Although some interviewees described Facebook as having been used more extensively for recruitment historically, with this subsequently migrating elsewhere ("I think in the early 2000s/2010s Facebook was big but…that has moved on and now it's more Instagram and Snapchat" - Interviewee 2), *Recruitment Pathway 2* below, for example, demonstrates that recruitment via Facebook continues to occur. Furthermore, one interviewee referred to LinkedIn, saying it had been used by exploiters for coordination purposes because, as a 'potential conduit…', it was unlikely to be detected. 'Technically', this respondent reflected, LinkedIn *could* be used as 'a means of…recruitment' (Interviewee 3), although they did not cite a particular instance or case involving children.

While LinkedIn was categorised as a potential recruitment tool, X was mentioned as a platform used more broadly by exploiters to post extreme views and content to engage and groom children who might respond (see *Recruitment Pathway 7* below).

The important conclusion, then, is that no digital platform is overlooked in relation to where recruitment and grooming might be taking place.

4.4 Children at Risk

Through our literature review, the Children's Society notes that **any child** can become a victim of exploitation but that **'there are patterns in the characteristics of children who are known to be exploited'** (2024:30).

In relation to CCE, in 2023, patterns of risk, according to The Children's Society, included mostly boys, with an average age of 15, an overrepresentation of Black and minority ethnic children (across all types of criminal exploitation), majority UK nationals (but with children who do not speak English or without immigration status particularly vulnerable) and with the extent and nature of the criminal exploitation of girls unknown.

In addition, children most likely to be affected by child criminal exploitation in the UK have been identified in the literature as those with histories of abuse, neglect, or trauma, looked after or care experienced children or those with unstable family environments, excluded pupils or those with persistent school absence, young people experiencing poverty or social deprivation, children with mental health difficulties or neurodevelopmental conditions, socially isolated children seeking belonging, status, or protection, children frequently missing from home or care settings and young people already exposed to gangs, violence, or drug markets.

Emergent research has evidenced some departure from this with evidence of exploiters, to avoid detection, targeting 'clean skins' where few if any of these potential vulnerabilities are in place. Shifts have also been noted in relation to girls and younger children being recruited into CCE. The Children's Society (2024) suggests girls are less likely to be identified, partly due to assumptions by police that boys are more likely to be criminally exploited and with girls more fearful of seeking help. Barnardo's (2023) notes, in its report to the APPG on CCE and Knife Crime, an increase in referrals of young girls affected by criminal exploitation into their service during the Covid-19 pandemic where they were offered 'significant amounts of money for drug running and county-lines activities.' Dixon highlights 'a key pattern' in CCE raised by practitioners of 'victims…becoming younger, with an increase in those aged 12 to 13' (2023:88).

The literature also highlights that exploiters deliberately target unmet emotional and social needs in children. Grooming commonly involves offers of friendship, money, status, safety, or 'family' to meet these needs before escalating into coercion, threats and violence.

In relation to the *online* recruitment of children into criminal exploitation, new empirical evidence from this research suggests that, while these factors largely remain relevant, the nature of online spaces extends the risk to include a *far broader* range of children. For one participant in our research, for example, trying to identify which children might be most at risk of online recruitment into CCE was misleading: **'That is the wrong question, because actually it's everyone…everyone's at risk because of the nature of what it is. And that's the problem'** (Interviewee 6). Another research participant said:

'…every kid has got access…they've got their phone…their tablets…they've got TVs. They're really clever in how…they can access things. It's their whole life…originally, we always used to say it was really vulnerable children, but I think it could be any child to be honest.' (**Interviewee 7**)

A third respondent commented on the well-known risk factors related to CCE which had previously informed her work:

'...questions for referral that we're always asking...what does their school attendance look like? Have they had any exclusions...any missing episodes? What is their family situation...have they had a parent in prison...are they a child who is in care...?' (**Interviewee 4**)

She was clear that CCE as manifest online does not always follow this 'textbook' approach and that more children were now potentially at risk:

'I think because of the online recruitment, any young person is at risk of criminal exploitation and we've supported... those young people who are recruited online, I don't think they are 'textbook'...in terms of the vulnerabilities we would normally look at...they come from affluent backgrounds, they have family at home...they go to school. So, all those normal indicators that we would look for...school exclusions or low attendance or a child in care...I think that goes out the window a little bit when we are talking about online recruitment...' (***Interviewee 4***)

This much broader range of children potentially at risk of online recruitment into criminal exploitation is extremely important for us to note.

In addition to highlighting that 'any child' might be recruited online into criminal exploitation, the research also identified risk factors with relevance in an online setting. These are set out in **Table 2** and expanded upon below, supported by evidence from the literature review, expert interviews and engagement with the LEAP.

Table 2: Risk factors for online recruitment into CCE identified through the research

Risk Factors	Detail	Literature Review	Interviews	LEAP
None	**'Clean skins' or 'any child' i.e., without any of the risk factors usually linked to CCE (see above)**	✓	✓	
Boys	**Online gaming, sexual extortion, financial exploitation**	✓	✓	
Girls	**Increasingly targeted online since COVID-19 pandemic**	✓		
Younger children	**Increase in those aged 12-13 due to social media access / phones**	✓		
Neurodiversity	**Autism, ADD, ADHD. Link to social isolation, SEND and school**	✓	✓	

School absence	**Lack of structure, supervision and time spent online, isolation**	✓	✓	
Socio-economic hardship, poverty	**More at home / online due to limited resources, family time or activities for youth. Need to earn money.**	✓	✓	✓
Loneliness	**Links to social isolation above**	✓		✓

Risk factors associated with online recruitment into CCE most mentioned through the research included boys (but also girls), younger children, neurodiversity, gaps in attendance at or exclusion from school, poverty and socio-economic deprivation.

Boys are considered particularly at risk of recruitment into CCE via, for example, online 'gaming sites' (Interviewee 11) (Palmer, 2015), to child financial exploitation (The Children's Society, 2025a) and 'particularly vulnerable to financially motivated sexual extortion' (Interviewee 1).

While far less specifically mentioned by respondents in our research, the NSPCC and Barnardo's, for example, note an increased targeting of **girls** in relation to CCE online. The NSPCC notes the 'disproportionate risks' faced by girls in relation to risks of harassment, abuse and exploitation online, relative to their male counterparts and with only 9% of (teenage) girls engaged reporting they feel safe online (2025:10). The NSPCC explores in detail the areas of digital platform design and digital features presenting risks to girls. It notes that online harm is predominantly conceptualised at the population level in research rather than understanding the specific experiences of girls and so it **'...takes as its starting point the fact that girls face a unique configuration of risks in the online world, differing in scale and nature to the set of risks faced by boys'** (2025:1).

For Barnardo's (2021), there has been a shift in 'victim type' in CCE with a greater reliance on girls, thought due to their increased access to and being targeted via exploiters on Snapchat and TikTok during lockdown.

Dixon explores 'victim trends' with residential care workers and other professionals working with children who have been criminally exploited in Scotland. While the **age** range reported by these practitioners ranged from 11 to 17 years old, with the most common ages affected being 13 to 16, a key pattern was that victims are becoming younger, with an increase in those aged 12 to 13. Participants suggested this decrease in age could be due to exploiters viewing these children as being less likely to be detected or, alternatively, to them having access to mobile phones and social media at a younger age (2023:88).

While the focus is on CSE rather than CCE, it is interesting to note here Palmer's finding for Barnardo's that the age of children at point of referral when the initial

concern is online abuse appears to be lower than that of children referred due to offline sexual exploitation. Workers reported children as young as 10, 11 and 12 years of age being more the norm (2015:31).

As part of our research, many respondents spoke about the risks facing **neurodivergent children** to online criminal exploitation, particularly children who are 'autistic', 'ASD' or 'ADHD', **'...children who...perhaps take things very literally, are lonely, struggle socially...'** (Interviewee 3) which can push them into online communities instead (Interviewee 4). In relation to online harm and child sexual exploitation, Palmer reports 'an increase in autistic young people being referred' to Barnardo's 'for internet harm' linked how these children 'perceive the world and relate with others' (2015:32).

Because of their greater social isolation, these children have been made more at risk also by recruitment into CCE manifesting online, as found in our interviews:

'Often, I see that it's disproportionately children who are neurodivergent that are targeted...neurodivergent young people tend to prefer to communicate exclusively online, and it's probably easy for the exploiters to pick up on cues sometimes if they're talking to somebody online.' (**Interviewee 5**)

Interview findings suggest that the risks associated with neurodiversity may intersect with those experienced by a broader group of children who struggle within mainstream education and, as a result, are excluded or absent from school, or placed on reduced timetables (Interviewee 11).

This closely aligns with Dixon's (2023) study of CCE in Scotland, in which professionals identified children **not being in mainstream education** as the most common risk factor, mentioned in 15 out of Dixon's 22 interviews. This included children who were not attending school or had been suspended, excluded, given alternative education or had a reduced timetable (which was also flagged in our interviews). Professionals felt that the lack of structure, supervision and protection usually provided by the school environment significantly increased these children's presence and visibility to exploiters online and their vulnerability to recruitment as a result. One participant from the Third Sector in Dixon's study commented:

'...they're being kicked out of schools, they're being excluded from schools, so they're like targets, you know? They're vulnerable young people that are on the street and they've got nothing to do with their time, they're on social media 24 hours a day, they've no break from it, they're just, they're prime candidates for these organised crime groups.' (**in Dixon, 2023: 83**)

Not attending school is a risk factor for online recruitment into CCE for a far broader range of children when it relates to school closures, for example in school holidays and at weekends (Barnardo's, 2023b). Barnardo's found that more than three quarters of children spend three or more hours online and one in five spend seven or more hours a day online at the weekend (2021:37). School closures during

the Covid pandemic lockdowns also had a significant effect. Barnardo's, once again, notes that the **'extreme sense of loneliness that many young people experienced during the pandemic resulted in many using a variety of social media platforms to establish and maintain connections'** (2023a).

One member of the LEAP was keen to stress that loneliness is a really important factor placing children at increased risk of recruitment into CCE online: **'it's not just about poverty!'** (Session 1, 25 February 2026). The LEAP also noted how children have increasingly turned to online communication as 'family time' and 'in person interaction' has decreased and as youth centres are closed (Session 1, 25 February 2026).

For one respondent in our research, children out of school, with a lack of supervision and affected by Covid combined with other related risk factors (for example neurodivergence, mental health issues) as well as the diversionary draw of online platforms, creates significant vulnerability:

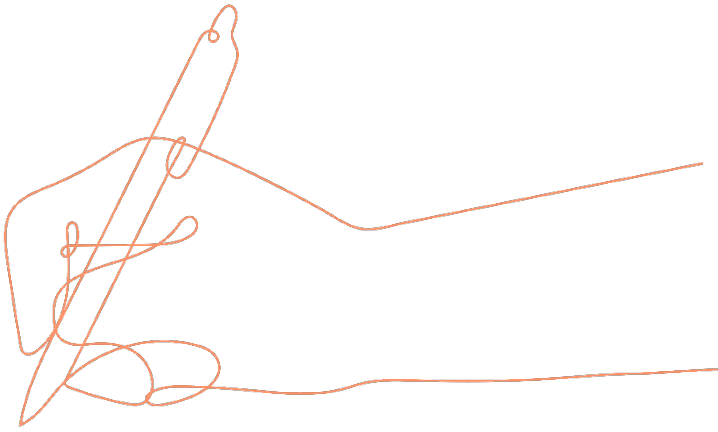
'...and those children in particular that are not in...education, the children that are struggling. And I think there's a lot of children that are neurodivergent or particularly the lots of young people who are anxious and not in school anymore as a follow up from COVID and as a sort of childcare mechanism or managing that child's mental health or that child managing that or retreating from it, there's a massive dependence on online gaming and a massive dependence on online. And obviously all of that then just escalates the risk.' (**Interviewee 11**)

Such non-attendance can interconnect with other risk factors such as a lack of parental supervision at home and/or parents' need to work longer hours due to financial pressures, increasing children's time spent online (Barnardo's, 2023b). The Children's Society also notes the importance of **socio-economic hardship and poverty** as drivers of child exploitation, citing how the **'cost-of-living crisis had exacerbated all forms of exploitation, youth violence and vulnerability, with one witness describing poverty, in itself, acting as a grooming process'** (2024:24).

Several respondents in our research also noted these drivers, including of online child criminal exploitation, mentioned in more detail in Recruitment Pathways 1 and 2. One respondent spoke about a lack of resources at both family and community levels:

'...children that probably have restrictions in terms of where...they can go...they don't have access to a proper play area. Maybe all they have is...their home and...due to restrictions or resources (not having enough of it), they're just...limited to their computers or to whatever they can access online...cost of living is going up. It's...expensive to go into a place and just sit and...you don't have to pay money for something...You would like to stay where you're spending less.' (**Interviewee 2**)

It is clear from the above that the risks of online recruitment of children into CCE are varied, complex and, in some ways, different to those normally associated with CCE including increasing cases where none of these risk factors apply. This makes identification of children at risk of and affected by online recruitment into CCE even more challenging.



[1] While not the UK, Sheehan, Walsh and Cusack (2024) explore CCE in the context of the Republic of Ireland. Despite an investigation into how young people are exposed to criminal activity in their communities, social groups and homes, however, there is limited exploration of the digital sphere. For example, young people's recruitment as drug 'runners' via social media is mentioned (2024:75) and a 'video confession' of criminal activity via Tik Tok (2024:271) but, while acknowledging that other 'studies have highlighted the role of social media in CCE', Sheehan et al. note that their young research 'participants did not raise the issue themselves' (2024:276).

[2] See for example Firmin (2017) and Firmin (2020) and also, to different degrees, Firmin et al (2022), Firmin and Lloyd (2022), Firmin, Lloyd and Bernard (2023), Firmin, Manister and Peace (2023), Wroe, Peace and Firmin (2023), Firmin et al (2024), Firmin (2024), Firmin, Peace and Wroe (2026) and Firmin (2026).

[3] https://www.childrenssociety.org.uk/what-we-do/our-work/preventing-child-sexual-exploitation/online-safety

[4] https://www.childrenssociety.org.uk/what-we-do/blogs/the-risks-snapchat-poses-to-children (Accessed 10 August 2026)

5: Findings: Mechanisms

The nature and design of digital platforms and the risk factors associated with certain groups of children and their circumstances provide important context for a consideration of the online recruitment of children into criminal exploitation and how this 'works' in practice. It is also essential to consider, within this context, the potential motivations, behaviour and actions of perpetrators and children as well as the recruitment methods and tactics exploiters employ. These are the mechanisms through which children can be identified, targeted and groomed into criminal exploitation. Some of these are already familiar to us from the extant research on CCE.

5.1 Recruitment Process and Tactics

Dixon (2023) describes the recruitment process into CCE and its recognised four stages. The first stage is the identification of a child, showing interest, offering gifts and status, building a relationship and isolating them, gaining their trust. The second stage tests the child's loyalty through an activity or errand, building further trust through protecting them from danger. The third stage gives the child more responsibility and involves a demonstration of their loyalty. The final stage 'traps' the child via threats, violence, humiliation and other forms of harm.[1] These stages have been drawn from those identified by The Children's Society, a 'target, test and trap' approach to grooming children into criminal exploitation (2019:8).

Dixon (2023) also sets out methods and mechanisms employed by exploiters as part of CCE: 'debt bondage', the use of violence, including sexual violence for control, peer recruitment and the glamourisation and normalisation of criminal activity and material wealth.

'Debt bondage' is a recognised tactic employed to coerce children into criminal activity. For example, the 'activity or errand' the child undertakes as part of the grooming process above will involve carrying something valuable (money, drugs etc). A robbery is then staged, or theft or arrest may occur, where this valuable item is lost and the child is then in 'debt' to the exploiter. Alternatively, a child may be unable to afford to pay for drugs provided for personal use, again creating a 'debt' and a form of entrapment. Such 'debt bondage' is not solely employed for 'county lines' related activity, also used where children have been recruited and then trafficked into cannabis cultivation in the UK, held responsible for the cost of their travel.

Intimidation, threats of violence, physical violence, weapons and kidnapping are used to recruit and control victims of CCE. Sexual violence is also often used as a means of intimidation and control, for example as punishment, particularly for girls who are being exploited or as a threat of harm to female siblings if boys do not comply with demands.

Peer 'recruitment' is when children who are being criminally exploited are coerced into 'recruiting' younger siblings or peers so exploiters can expand their networks and criminal activity. Children in the earlier stages of recruitment might perceive this as offering opportunities for making money and status to their friends.

The glamourisation and normalisation of criminal activity and associated violence as well as money, cars, jewellery and status – often via images and videos on social media - is mentioned throughout the literature on CCE and represents the earliest and most common recognition of how child criminal exploitation can manifest online. Less attention, as already noted, has been given in the academic literature to the online dimensions of other aspects of CCE.

Practitioners interviewed for this research enabled a deeper exploration of the digital aspects of recruitment into child criminal exploitation and how processes and tactics operated online.

5.2 Recruitment Pathways

Based on our research, we identified **ten online recruitment pathways** of children into criminal exploitation, set out in summary form in **Table 3**.

Table 3: Ten online recruitment pathways into criminal exploitation identified from the research

No.	Pathway	Description
1	'Easy money'	Exploiters send out mass messages to children promoting a job or opportunity to make 'easy money' and wait to see who responds.
2	'Have you got a passport?'	Exploiters post an online 'story': a job or opportunity requiring a passport and no travel restrictions and wait for a response.
3	New 'skins'	Children (primarily boys) participating in online gaming are identified through their basic gaming avatars and groomed via in-game chats.
4	'Buy now, pay later'	Children's access to drugs is quick and easy online and tactics such as 'buy now, pay later' create a form of 'debt bondage'.
5	'Images...as threats'	Children, primarily boys are coerced into sexual acts with peers or into criminal acts which are photographed / filmed by exploiters and used for extortion.
6	'A sense of belonging'	Exploiters target children online individually or in communities where there is some form of isolation and/or an unmet need for belonging.
7	Extreme communities	Exploiters target boys online through games or content related to extreme views and where there is isolation and/or an unmet need.
8	'Giving my bank details'	Children are groomed and coerced into withdrawing, holding or transferring money illegally.

9	Peer 'recruitment'	Exploiters (re)initiate or maintain contact online with looked after children moved 'out of area' and their peers if in residential care.
10	'Dating apps'	Dating apps are promoted online to children and used, despite age restrictions, by girls (and boys) who are isolated and seeking affection.

In keeping with the 'context-mechanism-outcome' approach of a rapid realist review, the following section articulates each pathway in terms of its context (both digital and in relation to children's vulnerabilities), common tactics and mechanisms employed by exploiters, and subsequent harms for children.

These pathways should be seen as evidence-based *examples*, in part composites and in no way the totality of recruitment into CCE online. They can and do intersect, interconnect, recombine and evolve.

The grooming process and its stages of 'target', 'test' and 'trap' (The Children's Society, 2019) and some of its tactics, for example 'debt bondage', are broadly similar across all pathways and familiar to us from the extant literature on CCE - with more 'open' initial contact with children online, then moving to more private and encrypted digital and/or offline channels and the creation of a 'debt' which fuels further exploitation. There are shared areas of multiple harm but also risks that are specific to some pathways and of course to different children, intersecting with their vulnerabilities. In each case, **we must be mindful that other digital platforms than those mentioned will be being employed, other children are being affected and other types of harm result.**

It is clear that the online recruitment of children into criminal exploitation is happening in multiple ways, and with significant harms for children and their lives.

Recruitment Pathway 1: 'Easy money'

Digital Platforms: Snapchat, Instagram, WhatsApp, Discord, Facebook, TikTok, Telegram

Risk Factors: Poverty and socio-economic deprivation, family instability (parental substance misuse), drug addiction, school exclusion or non-attendance, Not in Education, Employment or Training (NEET), neurodiversity

Mechanisms and Tactics: Exploiters send out mass messages to children promoting a job or opportunity to make 'easy money' and wait to see who responds. Responding child (and all their contacts) can be 'quick added' to an online group and/or communication moved to an encrypted channel where grooming takes place, leading to creation of a 'debt' ('debt bondage') repaid via 'county lines' (with meetups 'offline') or bank account fraud, other coerced criminal activity.

Harms: Debt, physical injury, criminalisation, stress and anxiety, psychological trauma, drug addition, further exploitation, impact on longer-term life chances.

Interviewees described how exploiters send out a 'scatter message', for example on WhatsApp, about a 'job' or 'opportunity' to make 'easy money' 'to hundreds and hundreds of young people' and 'wait and see who comes back to them' (Interviewee 1): **'…we get a significant proportion who are recruited online…through…different apps like WhatsApp or Snapchat or…Instagram sometimes, where it's…quite subtle and you see things like…want to earn some easy money…give us a message…'** (Interviewee 5)

Children identified as at risk of this recruitment pathway include those who are socio-economically disadvantaged, not in education, employment or training (NEET), with family instability or substance misuse and neurodiverse:

'…the tactics that we talk about…offering that quick cash…for lots of our children…not all of them…we're talking about children who are living in poverty, who haven't gone into education, training or employment opportunities…They are coming from familial exploitation…from families who are…entrenched in some of that behaviour. We are talking about children who are wanting to earn money, need to earn money, whether that's because they've got a drug addiction or for whatever other reason. We talk about children who…say that…their younger siblings haven't got X, Y and Z and mum and dad are drug addicts, or not around, and they're doing it for that. Why wouldn't they be enticed into earning a quick buck?' (**Interviewee 9**)

Dixon (2023) notes that such 'job adverts' circulated via WhatsApp can lead to children added to online groups to recruit them into 'county lines.' The Children's Society states that young people are targeted online via Instagram and then are **'told to meet at a random spot…this is where they're going to be get picked up…and they only get the screen name of the person that's coming…and then they'll get taken in a car…to the trap house or something.'** The harms associated with such 'county lines' activity 'offline' are well documented and manifold, considered 'acute, varied and long-lasting'. They can include 'physical and sexual violence, criminalisation, drug addiction, homelessness, psychological trauma and long-term effects on children's life chances' (The Children's Society, 2024:33).

Coercion into other forms of criminal activity can also result: **'Snapchat, for example, lends itself to…that kind of advertising: 'anyone make some quick cash?'…can we use a bank account, essentially'** (Interviewee 3). The Children's Society (2024:5), reporting on child financial exploitation including bank account fraud, notes that exploiters use social media posts, fake profiles and 'get rich quick' job adverts to draw children in via Instagram, Facebook (to a lesser degree), Snapchat, TikTok, WhatsApp and Telegram, then grooming children via private messaging to open/use bank accounts.

The Children's Society (2025a) sets out the harms from child financial exploitation. Children affected can experience intense stress and anxiety, can receive threats

and be subject to assault and other forms of violence and can go on to be further victimised and exploited. Other harms include being placed under investigation, not being able to open a bank account - which then impacts on their education, employment and future - and spending restrictions or frozen bank accounts for other members of their family.

Recruitment Pathway 2: 'Have you got a passport?'

Digital Platforms: Snapchat, Instagram, Facebook, Telegram, WhatsApp

Risk Factors: Looked after children. Poverty and socio-economic deprivation, family instability (parental substance misuse), drug addiction, not in school, NEET.

Mechanisms and Tactics: Exploiters post an online 'story': a job or opportunity requiring a passport and no travel restrictions. Responding child is 'quick added' to an online group and/or communication is moved to encrypted messaging where grooming takes place. A paid trip or 'holiday' overseas creates a 'debt' ('debt bondage') then used to coerce the child into trafficking cannabis into the UK from that location or across other international borders. Non-UK national children may be recruited (online) and trafficked into cannabis cultivation in the UK.

Harms: Debt, criminalisation, prosecution/imprisonment, death penalty, locked in properties, forced labour.

Two interviewees described another 'get rich quick' recruitment pathway where the job or opportunity advertised - via Snapchat, Instagram and Facebook 'stories' (24-hour disappearing videos and photos) - culminated in children being privately messaged on WhatsApp or Telegram and coerced into trafficking cannabis from overseas:

'...we're seeing quite frequently now...paying children to import drugs from Thailand and other places. And, in all those cases, it's been a...Snapchat 'story' or a Facebook 'story' about 'get rich quick' schemes. [--], on the ad, they ask them: 'Have you got a passport? Have you got any restrictions to travel?' because they apply for the visas and things for them. And then they pay for a week all-inclusive...as a result...they're indebted to them and they've then got to bring home a package...very large quantities of cannabis in a suitcase...back with them on the plane' (**Interviewee 8**)

One respondent stressed the escalation of this recruitment pathway: 'there must be about 15 or 16 in the last few months...' [Int 8], as well as 'looked after' children being those targeted most. Harms identified included criminalisation rather than protection: **'...they are charging under the importation offences...they're Schedule 4 offences...so we can't use the Section 45 defence...'** (Interviewee 8). And even more severe risks as this pathway evolves to avoid detection: **'...the exploiters**

naturally use a different method online now…getting them to take the drugs into Vietnam, where there's a death penalty potentially for these children' (Interviewee 10).

Dixon (2023) notes that the role of 'debt' in CCE does not always relate to 'county lines' nor solely to children who are UK citizens. The trafficking of children from overseas into the UK, with promises of money, a job or a better life, can lead to 'debt bondage' through being forced to repay the costs of travel through criminal acts including cannabis cultivation. 13 of 27 children who had been trafficked into the UK supported by the Scottish Guardianship Service had experienced 'debt bondage' by their exploiters. Children who are Albanian nationals in England and Wales and Vietnamese nationals in Scotland are increasingly criminally exploited via forced cannabis cultivation. While an online component of recruitment into such criminal exploitation is not made explicit here, it may well be involved in the earlier stages of recruiting children from overseas.

Recruitment Pathway 3: New 'skins'

Digital Platforms: Discord, PlayStation3, Roblox, Twitch. **Games:** Fortnite, Call of Duty, Grand Theft Auto, Cunch Chronicles, Drug Deal Simulator, FIFA, Valorant

Risk Factors: Boys, socio-economic deprivation, poverty, neurodiversity (autism), school exclusion / non-attendance, limited adult supervision, social isolation.

Mechanisms and Tactics: Children (mostly boys) (newly) participating in online gaming and/or with limited money, identified through basic gaming avatars, are groomed through in-game chats. Exploiters provide them with gaming credits, tokens, money for improving their avatar / gaming experience, creating a 'debt' ('debt bondage'). They are coerced into criminal activity (e.g., 'county lines', money laundering) based on this 'relationship' and 'debt'. Gamer tags and/or profiles provide information enabling contact 'in real life' and surveillance on and offline.

Harms: Debt, anxiety, poor mental health, psychological trauma, physical threats and violence.

A Barnardo's survey of over 20,000 boys and young men in the UK highlights the exploitation risks from gaming site chats (Palmer, 2015). Exploiters, it found, will chat to and groom boys while they are concentrating on the game and when their guard is down, encouraging them to share information and reveal personal details. Online gamer matching mechanisms, for example via PlayStation3, connect boys with unknown gaming partners online.

Respondents in our research also mentioned recruitment into criminal exploitation via gaming platforms, especially for boys. Interviewees particularly focused on the

monetised nature of gaming, how in-game costs and children's inability to pay create both a need and an opportunity for exploiters. One interviewee went on to describe this in detail:

'…when you create a gaming character for things like Fortnite, you have what's called a 'skin'. And when you first start a game, you have the basic… 'skin' and so it's obvious to all those other players…that you're a new person to this platform…and you haven't put any money into that game. And these games like Call of Duty, Fortnite…will always be prompting players to pay real money…so that they can get…better 'skins' and that creates an opportunity for perpetrators…they can start a chat with that person… 'I can send you money so you can upgrade your 'skin'…' And then we see those young people getting trapped in 'debt bondage' because that perpetrator will then turn around and say 'well, I bought you this and now you owe me.' (**Interviewee 1**)

Such 'debt bondage' along with information gathered by the exploiter from children's 'gamer tags' or in-game can lead to further harm 'offline': **'…it wouldn't take much for a perpetrator, particularly…in a gaming situation to…go…'what Year are you in…what school are you from'…as soon as they've got that…they can Google the area that child lives in and it won't take them long to find them from there'** (Interviewee 1).

Other (intersecting) risk factors identified in relation to this recruitment pathway included social isolation, school non-attendance and neurodivergence (including autism):

'…on the PlayStation and in computer games…I think those are the children that are potentially exploited through online, because some of those children could be a little bit more isolated, could be struggling going to school, could have things like neurodiversity, autism…it could literally start from an online…friend and they are from all over…Most people have got headphones on, you wouldn't know it's…going on…' (**Interviewee 7**)

As well as children struggling with mental health and/or parents struggling to cope and unaware of the risks involved: **'…lots of young people who are anxious and not in school anymore as a follow up from COVID. And as a…childcare mechanism or managing that child's mental health or that child managing that or retreating…there's a massive dependence on online gaming…'** (Interviewee 11).

The Children's Society (2025a:5), in relation to child financial exploitation, reports on exploiters approaching children via online gaming including on Fortnite, Valorant, Roblox, the FIFA, Call of Duty and Grand Theft Auto series or through online platforms linked to gaming, for example communities on Twitch. They note that exploiters offer virtual items – 'skins', 'mods', 'coins', 'V-Bucks' and transfer money to children online including 'rewards' to do things offline and build trust. Children become acclimatised to financial transactions via gaming exchanges and can be further exploited criminally and financially on and offline.

Dixon (2023) writes about children exploited through 'county lines', 'targeted via gaming platforms using the live game play function which allows exploiters to freely interact with children.'

Recruitment Pathway 4: 'Buy now, pay later'

Digital Platforms: Facebook, Snapchat, Telegram

Risk Factors: Substance misuse, debt, known peers or family members who use/sell drugs

Mechanisms and Tactics: Children using substances and seeking to buy drugs are exposed to mass marketing of drugs across online platforms targeted at children, including by people they know. Access to drugs is quick and easy online and tactics such as 'buy now, pay later' create a form of 'debt bondage' and coercion into drug-related criminal activity.

Harms: Drug addiction, debt, criminalisation, physical threats and violence.

In Walsh's (2022) research on CCE in Northern Ireland, all four young people's focus groups mentioned 'social media' for access to drugs and how 'dealers' used digital platforms to sell and exploit them. One interviewee in our research spoke about this pathway and how it evolves:

'I think that has been a way some of our young people have been recruited in mainly as a start off to access drugs and then once that's happened, there's some sort of hold or some debt that's owed and that turns into more of a physical thing…' (**Interviewee 4**)

For another respondent, pre-existing substance use - and associated cost - was a key risk factor and should be taken more seriously:

'I don't feel like we look at it enough…I've had professionals say to me: 'If we unpicked every young person that is using substances, they could all potentially be exploited!' I'm like: 'That is exactly what we're saying!'…if a young person was only using a '10 bag' of…cannabis a day, it works out something like £70 a week…young people don't have that kind of money' (**Interviewee 7**)

A hugely expanded and visible online 'market' where different emojis and icons are used to advertise drugs - 'definitely Snapchat in that respect' (Interviewee 4) and seeing 'who was dealing drugs, who was selling' via Telegram (Interviewee 8) - means children 'literally click a button' (Interviewee 7), providing exploiters with an easier route into making money and access to a wider group of children:

'…most young people have Snapchat…whatever it might be… it potentially opens up an absolutely huge platform…it's literally everywhere…pages where they are selling or dealing…just a constant thing…And I don't know how as a young person that you would avoid that because they are linked to people that you go to school… or…college with…' (**Interviewee 7**)

This recruitment pathway could also start 'offline' with children accessing drugs via QR codes posted around their neighbourhood 'that can just be scanned and that will put them directly in contact with the exploiter there and then' online (Interviewee 5).

'…that's probably the start of your recruitment…you've just seen them on lamp posts, just the QR code with a weed symbol. People just go into their phone, scanning it, buying it…your first step of someone identifying you as using substances and could potentially use you to supply them…' (**Interviewee 7**)

Dixon notes (2023) that 'debt bondage' can occur when children are given or buy drugs from dealers and accumulate a debt due to being unable to repay or afford them (National Crime Agency, 2019a; Ofsted, 2018). For example, interviews with victims of CCE and practitioners in Glasgow and Merseyside revealed drug dealers offer children drugs on a 'buy now, pay later' scheme, leading to drug-debts and being forced into drug dealing to pay this off (Robinson et al., 2019).

For one respondent, online exploitation via 'county lines' has long been an approach: **'…the online stuff is more…when they are being exploited and…how they're continuing that and how they're…networking with other…peers or people…and that's always been there, hasn't it, in terms of, like, 'lines'…'** (Interviewee 7)

Recruitment Pathway 5: 'Images…as threats'

Digital Platforms: Snapchat

Risk Factors: (Teenage) boys, peers subject to sexual extortion, engaged in criminal activity

Mechanisms and Tactics: Boys are targeted and coerced into sexual acts with peers or others or subjected to violence or forced into criminal acts which is photographed / filmed by exploiters and used as a threat to force them into (further) criminal activity ('county lines', fraud, money laundering, other) with online circulation of photos/films if they don't comply.

Harms: Shame and humiliation, stress, anxiety, debt, CIFAS marker, financial impacts, criminalisation, psychological trauma, sexual abuse and violence, physical injury.

There is significant literature - and substantial recent public debate - around child sexual extortion as part of online child sexual exploitation (CSE). The NSPCC provides case studies, including Snapchat, of 'sexual images' used by exploiters as threats to coerce money out of children (NSPCC, 2025; NSPCC, 2023). Barnardo's also share Snapchat case studies of the online sexual extortion of girls (B2, B3).

There is far less, however, on **criminally** (including financially) motivated child sexual extortion, a key mechanism in online recruitment into CCE where boys are considered more vulnerable:

'…boys are particularly vulnerable to financially motivated sexual extortion. [--] We're not entirely sure why it is boys that are so targeted, but the data that we get through from police forces and from the National Referral Mechanism…tells us that…overwhelmingly it's boys]' (**Interviewee 1**)

Dixon's (2023) study of CCE and 'county lines' highlights the role of sexual violence and child sexual exploitation, including online, to coerce and control boys into criminality. Exploiters are known to humiliate and shame children by forcing them to engage in sexual acts (e.g. kissing their friend, touching someone, etc.), then taking photos or videos of these acts and threatening to share them via social media if they do not comply. This pattern was also noted by a respondent in our research:

'…a lot of…groups around…are shaming young boys…they're taking videos of them doing sexual acts, or violence against them where they're getting upset and…they're then posting those online to control the young person…to keep them in check, to keep them being exploited.' (**Interviewee 8**)

Children are not solely coerced into 'county lines' through online sexual extortion, however. The Children's Society has reported on how child financial exploitation can involve sexual extortion as a tactic and means of control, where children are coerced into transferring money between bank accounts for fear these images will be exposed online (2025a:5). In addition to the shame, anxiety and fear involved, additional harms relating to financial exploitation can include a CIFAS marker,[2] poor credit record, frozen bank accounts (including of family members or peers) and long-term effect on opportunities and career.

Another respondent in our research noted that the criminal activity a child may be coerced into can be the online sexual extortion of *other* children:

'…a child…sexually exploited online, adult male groomed him…was then directing child to obtain other child sexual abuse material from other children…so, in effect, he was criminally exploiting that child online. But of course, once that happened…if child said they wanted to stop: 'Well, no…you're in too deep now. If you do, I'm going to send all these messages to the police.' (**Interviewee 3**)

Criminally motivated extortion may also not be sexual in nature and can be broader:

'Any kind of images can be used as threats…any kind of conversations or evidence around, you know, any criminal activity, they'll…use that as well…a young person that maybe has…gone and robbed a shop or caused criminal damage at the say so of the exploiter, they're not going to necessarily think that people are going to be supportive if they come forward and talk about it.' (**Interviewee 12**)

The harms caused by the sharing of these images is significant, including stress, anxiety and other emotional and mental health impacts on children. As one respondent outlined: **'it's completely life changing for these young people'** (Interviewee 1).

Recruitment Pathway 6: 'A sense of belonging'

Digital Platforms: Instagram, Snapchat

Risk Factors: Social isolation, lack of trusted adults, neurodiversity, poor mental health, lesbian, gay, bi-sexual, transgender and questioning (LGBTQ)

Mechanisms and Tactics: Exploiters target children online individually or in digital communities where there is some form of isolation and/or an unmet need for acceptance, affection or belonging or exploration of (shared) aspects of their identity. They meet this by providing online 'friends' or befriending children (posing as understanding adults or as children with common experiences).

Harms: Abuse of trust, trauma, criminalisation, 'outing' of sexuality / identity and related exposure and associated harms, threats, coercion.

Grooming as exploiting children's need for acceptance and belonging is well documented. Research respondents were clear that this 'vulnerability' was also being exploited through recruitment into CCE online: **'...a sense of belonging...that's commonly what we see with...organised crime groups ...where it becomes a 'family'. So those without...love and affection and care...then look for that belonging and affection elsewhere'** (Interviewee 3).

This 'mechanism' is common to many of the online recruitment pathways set out in this report. One specific digital tactic highlighted as employed by exploiters to meet this need was providing children with online 'friends': **'...it was a thing a couple of years ago where...for sort of being part of a gang...they were rewarding you by having loads of 'friends' on your Instagram and your Snapchat and stuff, in order to boost your popularity.'** (Interviewee 8). Certain children were considered by respondents as being more at risk in this regard than others:

'...when there is instability or if there is some sort of lack, or a gap, in their needs being met, that is what would make them more vulnerable. So, say...children that don't have a strong social support system, you know, where...they're not able to form meaningful, trustworthy relationships with the...adults around them. They don't have like a friend circle that they can go to...they tend to be excluded, so then they...go into groups where nobody knows anybody and then, you know, you can sort of just say what you want and that kind of is a good way to build community, but it also makes you really vulnerable to people that don't really mean well to kind of take advantage of that.' (**Interviewee 3**)

In several cases, these risk factors were related to neurodiverse children and perpetrators deliberately exploiting this need for belonging through their approach online:

'And I think it pushes them into the community more and especially online…They don't understand…those perpetrators who are contacting them online. They're just after some sort of status and friendship…some form of being part of something. And I think that makes them really susceptible to exploitation both…in person but online as well. And I think again access online to those young people is made a lot easier in those ways. So definitely something we are now including as part of our usual screening.' (**Interviewee 4**)

Palmer identifies groups of young people seeking social interaction and belonging online as more at risk of exploitation, for example those with poor mental health and lesbian, gay, bi-sexual, transgender and questioning (LGBTQ) young people (2015:7). Respondents in our research also flagged the vulnerability of children trying to 'figure out their identity', including in relation to their gender and sexual orientation, through a group or community online as well as the risk of criminally motivated extortion based on threats of exposing these aspects of their identity widely online.

Recruitment Pathway 7: Extreme communities

Digital Platforms: Discord, Call of Duty, Facebook, Instagram, X, Telegram

Risk Factors: (Teenage) boys, mental health and body image disorders, neurodiversity, self-harm, exploring sexual orientation and gender identity, history of sexual and/or physical abuse, substance misuse

Mechanisms and Tactics: Exploiters target boys online through games or content related to extreme views and where there is isolation and/or an unmet need for acceptance, status, belonging. They engage them in an online 'community', increasingly exposing them to harmful content and coercing them into extreme and/or criminal activity 'offline' which is recorded and shared online, creating further harm.

Harms: Radicalisation, extremism, criminalisation, violence, self-harm, exposure, suicide, arson, serious sexual and physical assault, murder.

There are many different online communities including those associated with extreme behaviour and views. Children, particularly boys, are being targeted by exploiters through connecting with or responding to content from such groups, for example relating to racism, fascism, homophobia, misogyny (and 'incels') and different forms of violence.

Radicalisation is considered a form of exploitation, and in many cases, overlaps with criminal exploitation when individuals are coerced or manipulated into committing extremist or terrorist acts. In some of the cases discussed in

interviews, practitioners had made referrals to Prevent, the UK Government's initiative addressing vulnerabilities to extremist influences, preventing radicalisation of individuals and terrorism through early intervention and support. For one respondent, the risk factors leading to radicalisation and to criminal exploitation in the early stages were 'very similar': 'they get led down different paths. But it seems to be the same almost driving factors at the beginning' (Interviewee 11).

One example provided of a platform where such engagement was happening was Discord:

'…with your extremism cases, which we're seeing more and more…the number of Prevent referrals I've done the last three, four months is unbelievable in terms of right-wing extremism, it's quite shocking…a couple of incel…referrals for young people as well…There's so much online on Discord and…those sort of like chat…information things…' (**Interviewee 8**)

Gaming platforms and military video games series like Call of Duty were also mentioned as an entry point for exploiters:

'Call of Duty especially…I've seen that on a couple of children…which have led to Prevent referrals…they've got certain groups on there, which may have…a tag name which is racist or…homophobic…luring the child into that…with gaming platforms…it always goes on then to the more encrypted…messaging platforms…' (**Interviewee 8**)

Beyond this, social media platforms were identified as locations where exploiters would connect to and/or share extreme content, groom and coerce children into violent and criminal activity.

The relatively recent development of online communities known as 'Com' (Community) Networks, predominantly, but not always, engaging males between the ages of 14-17, are of significant concern and involve multiple serious harms. A jointly authored alert from the NPCC, NCA and Counter Terrorism Policing from earlier this year defines these groups as: **'Transnational Virtual Networks (TVN) of criminal actors which engage in a variety of illegal acts or coerce others to do so in furtherance of their own personal gain, development of their infamy or in furtherance of their ideologies'** (Counter Terrorism Policing, NCA and NPCC, 2026:3).

Harmful behaviours Com Networks are engaged in include sexual extortion of young people (often but not exclusively of females), coercing them into self-harm and suicide and into recording or livestreaming these acts, then shared within the Networks, cybercrime and violent criminal acts 'offline' (arson, serious sexual and physical assault, murder) which can be targeted or indiscriminate.

Those targeted by these Networks are often, but not always, children, identified via online forums providing help and advice for mental health and body image

disorders, neurodiversity, self-harm and suicide, sexual orientation and gender identity, sexual and/or physical abuse and substance misuse. The alert warns of this 'emerging threat', noting that Com Networks 'primarily operate on Discord and Telegram' but: 'are active on virtually all social media and online gaming platforms.'

One respondent in our research spoke at length about Com Networks: **'It's an incredibly disturbing trend…groups, primarily of young people online…taking part in a lot of different dangerous behaviours, so we've seen examples of…extreme right wing, extreme bigotry, extreme racism, bestiality…forcing others to self-harm. And we're seeing evidence of criminal exploitation in there as well'**; and concluded: **'…everything wrong with digital spaces is taking place in these groups'** (Interviewee 1).

Recruitment Pathway 8: 'Giving my bank details'

Digital Platforms: Instagram, TikTok, Snapchat, online gaming platforms

Risk Factors: Boys, poverty or socio-economic deprivation (but not always), debt from substance misuse or excluded from school, neurodivergence, refugees or migrants.

Mechanisms and Tactics: Children are groomed via their social media accounts and on gaming platforms and coerced into withdrawing, holding or transferring money illegally, digitally (including cryptocurrency) and/or 'offline', either as a single instance or cumulatively over time. This can evolve into other forms of criminal activity.

Harms: Criminalisation, debt, damaged credit record, frozen bank accounts, CIFAS marker, long-term financial implications, anxiety, stress, trauma.

Respondents were concerned about online recruitment of children into financial exploitation, a more 'hidden' form of criminal exploitation. A child might think: **'I'm not technically…doing anything wrong. All I'm doing is…giving my bank details, withdrawing money from an account or transferring it somewhere…'** (Interviewee 3).

The Children's Society (2025a and 2025b) has published two reports on child 'financial exploitation', an under-identified type of child criminal exploitation defined as: **'…a form of child abuse that occurs when an individual or group takes advantage of an imbalance of power to encourage or compel a child under 18 to undertake a financial activity that benefits the perpetrator or facilitator'** (The Children's Society, 2024 in 2025a).

Children vulnerable to this form of CCE are often male, experiencing poverty or socio-economic deprivation (including where their families are involved) but also children from more wealthy families are also targeted (they have bank accounts!).

Children who are in debt from substance misuse or excluded from school, neurodivergent, are experiencing pre-existing exploitation or are refugees or migrants (The Children's Society, 2025a) are also at risk.

The UK Government (2024) defines 'money laundering-linked financial exploitation' as including 'physical cash and/or payments through financial products, such as bank and cryptocurrency accounts.' Child financial exploitation, then, can take place both offline and online.

The Children's Society (2025a) found that some of the methods involved in children being coerced into laundering money (including from the sale of illegal substances) through their online bank accounts 'mirrored those employed for other forms of child exploitation'. They involved online encounters and 'relationship' building via social media accounts or online gaming platforms' and offline methods were also used. Online recruitment platforms and pathways related to child financial exploitation are exploiters posting fake job adverts, financing children's gaming and sexual extortion, akin to and included in our Recruitment Pathways 1, 3 and 5 above.

One respondent in our research suggested that financial exploitation is a more hidden and prevalent form of CCE:

'…financial exploitation…is something that…I strongly suspect is happening more online than we are identifying and probably because, sometimes, some of those instances very much are a one-off instance of exploitation, perhaps no one ever really knows that that's happened…your child protects it particularly well or your bank doesn't pick up on suspicious activity or parents, or wherever, don't have oversight of that bank account or what that looks like.' (**Interviewee 3**)

The same respondent spoke about an example where cryptocurrency had been used, whether as a 'reward' for a child to coerce them into criminal activity or an online cryptocurrency transfer being the criminal activity itself: 'a tool or a purpose for exploitation online' (Interviewee 3). Another respondent said he'd seen 'a lot of financial exploitation…online currently as well' (Interviewee 8) and provided an example of where exploitation had begun offline, with a child coerced into stealing cash from his parent's account to 'invest' for a greater return and then, later, access to that account by the exploiter with transactions moving online.

Participatory research with young people about financial exploitation (The Children's Society, 2025b) found that 'scam' posts were commonly encountered across social media platforms such as Instagram, TikTok and Snapchat, often promoting aspirational lifestyles - fast cars, expensive jewellery – or opportunities for 'quick cash.' Young people felt such approaches could appear more credible when associated with influencers, verified accounts, or those known to the young person in real life or online. Direct approaches from seemingly trustworthy individuals (such as, another young person or a woman) could increase the

likelihood of engagement. They also highlighted how financial exploitation could spread through peer networks following successful transfers, or through threats and intimidation, although some reported that exploited young people might avoid involving friends for fear of putting them at risk. Others felt that young people experiencing financial exploitation wouldn't tell their friends or ask them to do it so as not to put them in danger. Young people were generally unlikely to report suspicious posts, believing that platforms or authorities would be unlikely to respond.

Recruitment Pathway 9: Peer 'recruitment'

Digital Platforms: Instagram

Risk Factors: Looked after children including those in residential care facilities and moved 'out of area' into an unfamiliar setting/location. Lack of / unmet need for family, belonging, affection. Debt, poverty or socio-economic deprivation.

Mechanisms and Tactics: Exploiters (re)initiate or maintain contact online with children who are moved 'out of area', identifying and locating them via social media channels or on gaming platforms where contact has been lost. Where children are placed in residential care with other looked after children, exploiters can coerce them into recruiting other children from these care settings.

Harms: Re(exploitation), criminalisation, threats, intimidation via surveillance, violence.

Looked after children and their peers in care settings can be vulnerable to CCE as noted by Dixon (2023), Maxwell and Wallace (2021) and others.

There is evidence that exploiters will re-ignite contact or retain communication online with looked after children when they are moved 'out of area', a practice known to increase vulnerability to child criminal exploitation. For example, Dixon cites research where 71% of 41 police forces responding to Freedom of Information requests stated that placing looked after children out of area increased their risk of exploitation (All-Party Parliamentary Group for Runaway and Missing Children and Adult, 2019), including through maintaining links with exploiters via technology and social media and being coerced into 'recruiting' other children from these care settings (2023:26).

Maxwell and Wallace (2021:45) also comment on looked after children placed 'out of area' as well as parents' attempts to relocate children away from exploiters and harm. However, numerous examples were given by parents of exploiters contacting these children including meeting them outside residential care homes. Parents suspected contact was maintained via their mobile phones or gaming communication channels.

Respondents in our research also commented on the vulnerability of looked after children in residential care homes to recruitment online:

'…if we have young people who live in care homes who are…a little bit more vulnerable and don't have those safe adult networks around them as much. That's a group of potentially very vulnerable young people in…very close proximity.' (**Interviewee 1**)

This pathway demonstrates how children who might previously be out of reach of exploiters can be (re)recruited and further exploited through digital means.

Recruitment Pathway 10: 'Dating apps'

Digital Platforms: Snapchat, TikTok, OnlyFans **Dating Apps:** Omegle, Tinder, ooVoo, MyLOL, Grindr, Wizz

Risk Factors: Girls (but also boys), low self-esteem, unmet need for affirmation and affection, socially isolated, loneliness, socio-economic deprivation and poverty.

Mechanisms and Tactics: Dating apps are increasingly promoted via social media to children and used, despite age restrictions, by girls (and boys) who are isolated and/or seeking affection and affirmation online. Individual children are targeted by exploiters (posing as children or younger adults) via these apps and coerced into sexual and criminal activity including through criminally motivated sexual extortion.

Harms: Emotional and psychological harm, violence and sexual violence, humiliation and shame, exposure, criminalisation.

One of our respondents spoke about a girl who had been groomed online into CSE, and the risk of low self-esteem and seeking affirmation from others which can be exploited by perpetrators online:

'…some of the cases that I'm working with, sexual exploitation…young people who really suffer with self-esteem…it's really common for young people to put a lot of…status on how many Snapchat 'friends' you have, how many followers you have…how many views do you get on your TikTok video…this particular young person…she's got very low self-esteem…negative history in relationships…she's very, very open on her settings and I think she's seeking that affirmation from males…it's very easy…to exploit them and…you can create any profile you want…pretend you know somebody from that area.'
(**Interviewee 12**)

In 2013/14 Barnardo's aired concerns (based on its annual survey about boys) about CSE and Grindr (Palmer, 2025). In its 2023 submission to the *All-Party Parliamentary Group on Child Criminal Exploitation and Knife Crime*, Barnardo's practitioners reported a surge in the use of online dating apps by under 18s during the initial lockdown period during the Covid pandemic, which facilitated both CSE and CCE. An increase in the use of dating apps by children and young people

included sites such as Omegle, Tinder, ooVoo and MyLOL, with 7% of Tinder uses being 13–17-year-olds at that time, although since further regulated. Barnardo's notes that TikTok and other social media are renowned for heavily promoting the use of dating apps amongst children and young people, seeing younger influencers encouraging children to use these adult-centred apps. Although age restrictions are in place on dating apps, they are easily overridden, vastly increasing the risk of online child exploitation.

One respondent in our research mentioned children's use of '…the Wizz app and these dating apps…' (Interviewee 7). Another respondent commented on how children were selling 'feet pics' online, initially via OnlyFans but since transitioning to other sites:

'…one thing I've seen recently as well is a lot of children selling feet pics…in terms of…OnlyFans and the other ones, they're so heavily regulated now, children can't go on there, they need so much ID, but…there's a feet pic site…they're going on that…and being made to sell pictures of their feet. And the amount of money people are paying on that but then there's different things then that will go on then. So that's like, it might be a game, or you can make 20 pounds selling a tour of your feet, but it's then, once you're in that cycle, then…' (**Interviewee 8**)

This pathway further reinforces how recruitment pathways adapt and evolve as well as the need to consider the intersectionality of CSE and CCE in relation to the online recruitment of children into criminal exploitation.

[1] This process can be further sub-divided, for example as in the Gap Analysis accompanying this report, into 1) targeting and identification 2) contact and relationship building 3) grooming 4) testing and initial involvement 5) exploitation and control, entrapment and 6) continued exploitation

[2] A CIFAS marker is applied by a financial institution or other member organisation when there is suspicion of fraud or misuse of financial services. It serves as a warning to other institutions about potential risks associated with that individual, helping to prevent further fraudulent activity
CIFAS stands for Credit Industry Fraud Avoidance System linked to the National Fraud Database (NFD)

6: Findings: Outcomes

6.1 Harms to Children

The recruitment pathways set out in Section 5 evidence multiple and intersecting forms of harm to children. They also demonstrate that the *type* of child criminal exploitation is significant in relation to the different harms involved. Harms specific to, for example, financial exploitation and criminally motivated sexual extortion are outlined in more detail in Recruitment Pathways 8 and 5. However, whilst identifying certain types and patterns of harm, respondents in our research were also keen to stress that different children could be differently impacted by online recruitment into criminal exploitation. If you spoke 'to 100 professionals…they would give you 100 different answers' based on the harms children supported had experienced (Interviewee 1).

The Children's Society states that 'the harm that results' from child criminal exploitation is 'acute, varied and long-lasting. It can include harms related to physical and sexual violence as well as drug addiction, homelessness, psychological trauma and long-term effects on children's life chances.' (2024:33) Barnardo's notes that such exploitation is 'too often misunderstood, and children can be blamed for their own abuse - in some cases being criminalised rather than offered support.' (2023:2)

The negative outcomes of CCE are well-documented and manifold. The *Criminal exploitation of children, young people and vulnerable adults – county lines* (UK Government, 2023) sets out a range of harms connected to criminal exploitation including physical (injury, serious injury or death from violence, sexual violence, internal concealment of drugs, substance dependency or overdose), psychological and emotional (trauma, fear, stress, anxiety, self-harm, depression), social (isolation, breakdown of relationships, overdependence on exploiters), developmental (disengagement, impact on future prospects and opportunities, disrupted development), material (exposure to unsafe environments, debt) and legal including arrest, criminalisation and criminal records. CCE can also compound pre-existing disadvantages as well as generate new areas of harm.

There is, however, limited investigation and understanding of the harms caused by child criminal exploitation online.

Participants in our research spoke about professionals' confusion over CCE online - they 'don't know where this sits' (Interviewee 7) - as well as a misrecognition of its severity and the harm involved:

'…sometimes perhaps we feel that young people are safer if it's, I'm…going to say 'just' online very loosely…Because there's not that…immediate physical…risk there, maybe it is downplayed…' (**Interviewee 12**)

This then impacts on the identification of these children and their referral for support, despite some such cases having been recognised to date under the NRM:

'…if it's just online concerns that we'd have, I don't know if that would be enough locally to…flag the screening tool, for that to be considered, you know, solely online exploitation…' (**Interviewee 4**)

Children themselves often do not know they are being exploited and are not aware of the potential harms involved. The Children's Society notes that children are particularly unaware of financial exploitation (2025a) and that children consulted on this said that they had heard nothing about this form of exploitation at school (2025b).

Participants in our research, however, described the escalation or 'slippery slope' of child criminal exploitation as it evolves 'further into drugs or other forms' of harm (Interviewee 3). They note the harm to children from the 'massive impact of trauma' (Interviewee 1) related to online power dynamics, coercion and threats and their cumulative effect on their mental health and well-being, for example: **'…the exploiters were sending images of a young person being sexually assaulted and saying: 'This is what happens if you don't do as you're told.'** (Interviewee 5) and **'…threats ranging from…physical wounding, stabbing…there's no limit to the kind of messages like that that you can get online'** (Interviewee 3). Such threats created fear, stress and anxiety for children, further exacerbated via digital surveillance and control:

'And just the presence as well…messages like 'Oh, I saw you there earlier' or '…what you up to? I thought you were doing this', that kind of level of intrusion into somebody's life, so that they feel the exploiters are always there…always know what they're doing and there's no escape.' (**Interviewee 5**)

Dixon (2023) draws on research on CCE in Glasgow and Merseyside to show that such threats soon went to physical violence, as well as children being locked into premises. Respondents in our research also spoke about where online threats turned to violence and physical injury and harm: 'we have had serious significant incidents where our young people have been attacked' (Interviewee 4); **'young people can be forced to harm themselves' and 'can be forced to harm others'** (Interviewee 1).

This violence and the resultant level of harm could depend, in part, on where the child was 'positioned' within an Organised Criminal Group. As one respondent commented in relation to children more entrenched in criminal exploitation:

'…the level of risk that they are subjected to is massive. And we've seen, you know, machete attacks, horrendous things that our young people are subject to and when it gets to that point, they just do not see any way out…it really feels that hopeless.' (**Interviewee 4**)

For one interviewee, an online normalisation of violence and criminal activity worked to 'desensitise children' (Interviewee 12) and against them recognising the

harms involved, as did their tendency to blame themselves: **'…predominantly, our young people, we see them as victims first and foremost. But…they don't understand or appreciate that it is exploitation. And I think that is the hardest message for them…'** (Interviewee 4).

Others referred to how some children withdrew socially and from any digital engagement after experiencing recruitment online - 'he went in on himself a lot…he was very introvert. He didn't speak' (Interviewee 4) - also impacting their mental health:

'…they refuse to go back and set up an online account…they just take themselves out of that space…Short-term impact obviously is…losing touch with your social group… if you're at school, not…doing very well in the learning…side of things…feeling isolated or worried and stressed, overwhelmed, anxious…' (**Interviewee 2**)

For Walsh and Harland (in Walsh, 2023), we need to better understand the prevalence and nature of harms related to CCE in different contexts from the perspectives of children themselves. This is also the case for harms caused by CCE online.

6.2 Mitigations and Interventions

The prevention, identification and mitigation of any form of child exploitation is challenging given its extent, sensitive and complex nature. This challenge proves even greater where child criminal exploitation online is concerned. As previously mentioned, online recruitment into CCE occurs across multiple digital platforms, through intersecting pathways, employing diverse tactics and mechanisms which evolve over time. Limited attention, as shown, has been given to this problem and those children affected in the academic literature, let alone to its mitigation. While there are potentially relevant examples of mitigation approaches relating to online CSE, much of this section focuses on views and ideas from our interview respondents on platform-level and other forms of mitigation. A clear message is that a system-wide approach is needed which includes meaningful and ongoing interaction between safeguarding and digital experts and children with lived experience.

'Ill-equipped to protect'

The Children's Society states that we 'are ill-equipped to protect and respond' to child criminal exploitation online. We 'don't have the knowledge or the tools to tackle this effectively' (2024:8). Practitioners interviewed for our research felt similarly ill-equipped to deal with online recruitment into CCE at the required speed and scale:

'…we are constantly on the back foot in terms of being able to address, being able to disrupt, being able to challenge and safeguard those children from…that online

grooming and method of attracting them…it's always 'after the fact' (Interviewee 9).

This research sought to explore potential mitigations at digital platform level that might address such online recruitment. However, some respondents struggled to identify such interventions, for example: **'I think they are trying, but kids know how to get around stuff, they just make new accounts…I haven't seen anything that particularly works, massively'** (Interviewee 7) and **'I can't think of a single example…any kind of online platforms doing something that would actually be helpful or beneficial in keeping people safe'** (Interviewee 1).

A few practitioners could come up with some good practice at platform level. For example, one noted that 'Roblox have got very…switched on' to recruitment taking place on its platform and are 'educating professionals' on risk management (Interviewee 8). Others mentioned Instagram as enabling linking 'to a parenting account' (Interviewee 7), reporting an account (Interviewee 2) and making some improvements in safeguarding and 'content indicators' (Interviewee 4). TikTok was seen to be 'trying', in requiring under 13s to have 'a parent in the background at all times', and TikTok also required a child to upload 'documents if they question your age' (Interviewee 7). One respondent said Snapchat blocked the unique identifier (MAC address) of any phone reported as being used to advertise drugs on its platform so that Snapchat could not be accessed via that phone again (Interviewee 8). The same practitioner reflected further on this 'good deterrent' and how 'if you started doing that with exploiters' it could get 'quite pricey' for them. The same blocking tactic could potentially be used for Roblox and Xbox, while digital gaming platforms would be more of a challenge as in-game chats are not currently monitored.

Others were sceptical about the degree of buy-in from big international companies to address the online recruitment of children into criminal exploitation in the UK:

'It's so difficult to get these bigger platforms to do anything about it, and particularly when a lot…of the headquarters are based overseas and…a lot of them are owned by Meta, for example, and trying to get in contact with Meta to put something in place to protect young people is next to impossible because, as far as they're concerned…why do we care about a child in the UK?' (**Interviewee 1**)

Specific instances were mentioned where action had not been taken by digital platforms to address harm to children, for example where 'young kids' known to a practitioner had 'put up promotional stuff with knives' (Interviewee 6) but, despite his efforts, the companies had not taken it down. The LEAP (Session 1, 25 February 2026) felt that digital companies should be made responsible to trace disappearing & encrypted messages ('it's evidence!') and that they needed to monitor content, take harmful content down and that progress against the Online Safety Act needed to go faster. One LEAP member suggested a 'digital forensics

team' or teams able to trace evidence and track digital pathways into exploitation. One person interviewed for the research commented, by association, on Ofcom and questioned the degree of pressure and influence the regulator had over digital platforms – 'they haven't actually got any teeth': **'I haven't seen anything from Ofcom…showing me that they're any use or any value whatsoever…they're not actually going to do anything…'** (Interviewee 6).

Some respondents spoke about what, at the time of interview, was a *potential* social media ban for under-16s in the UK[1] and had varied views. One interviewee felt that a ban was essential given the inaction by digital platforms to date:

'…making the organisations responsible for putting out stuff…have a social media contract with the government. …They will put proper age restrictions because New Zealand did it. And of course, some kids can get around it…setting up a VPN is actually very easy to do…but the vast majority of people just say, 'well, no, I don't want to break the law'… And the adults have to do it because if the internet companies were going to do this, they would have done it a long time ago, if they really cared…' (**Interviewee 6**)

Others were sceptical whether it could work, thought platforms and exploiters should be the focus, not restrictions on children, who would find (less safe) ways around the ban, or it would lead to unintended negative consequences:

'I just think technology is changing at such a fast rate. I just can't see how it can be regulated and be safe…even if we ban social media for children, it'd be more dangerous…we've allowed children to become used to social media…the online world is just as important to our children now as the physical contact…we've allowed social media to become such a big part of their lives…' (**Interviewee 8**)

These practitioners, working at the 'frontline' to disrupt online child criminal exploitation are drawing on the resources they have and can find but are calling for support. They are close to the problem and the children affected and essential for solution generation but cannot do this alone.

An ecosystem of actors

While respondents felt that digital platforms had a deep and urgent responsibility and a significant and much-improved role to play, they explored responsibility more broadly, looking across an ecosystem of actors to think about where mitigations might work. This included themselves and other professionals working with children, parents, teachers, academics and researchers, safeguarding and technology specialists and experts, youth workers and mentors and, most importantly, children themselves.

Respondents started with their own and other professionals' practice and the need to fully embed the digital dimension in their work, for example in safety planning with children. In this activity, the online world could be 'glaringly absent' (Interviewee 10), 'we just completely…avoid it…don't even mention it' (Interviewee

7), 'I'm missing everything online' (Interviewee 8). In part, this was because their safeguarding 'training, knowledge, expertise and experience' to date had 'been about something very different' (Interviewee 11). Some had started to address this: **'I always do an 'About Me'…But now I've incorporated an online version of that… 'Who are you talking to online? How long have you known them?'… it's probably one of the first things I say when…I'm looking at this child's relationships. I always head towards the online'** (Interviewee 8).

A couple of respondents mentioned the *Barnardo's Online Risk Guide*[2] co-created with *ParentZone*, practitioners and young people, and used it in their work to provide guidance on the risks and harms of going online. Alongside this guide, Barnardo's have established an online Community of Practice where people can share experiences and learning and stay informed about developments in online safety. Such a community may have the potential to be built upon to further enable a dynamic and responsive knowledge base and support for practitioners on online exploitation and harm. For one respondent, guidance and support also needed to come to practitioners from above: **'…it's a strategic issue… it needs to come top down…about the importance of online safety…if you look at the Home Office disruption toolkit…where…does it mention disruption in the online world? We haven't kept up with the challenges that are vastly evolving…'** (Interviewee 10).

Practitioners were, however, keenly aware of the expectations on and challenges for parents and carers, despite online guides on 'keeping your child safe' and 'setting up restrictions'. Parents, said one respondent, 'are lost…even with guidance' - which is often 'not very user friendly' (Interviewee 8) - and cannot be 'that safeguard' since they are often 'less equipped than professionals to understand' the risks and to 'really take action' (Interviewee 11). Safeguarding leads in schools, suggested another respondent, should be able to be 'first responders', identifying and referring pupils at risk of online exploitation, with schools 'critical to understanding the online experience' of children (Interviewee 10). However, for one respondent, building digital literacy and online risks into the curriculum when children 'first start school' and underpinning education 'all the way through' rather than relying on certain teachers, IT lessons or standalone modules was the way to proceed to tackle online harm (Interviewee 11). For the LEAP (Session 1, 25 February 2026), awareness raising on online recruitment into CCE in schools was essential and they also flagged the importance of banks collaborating across the UK with a red flag system to protect children from money laundering and bank account fraud.

Practitioners recognised what had worked for them in the past in terms of multi-stakeholder collaboration and coordination, responding quickly and early to emergent risks to children. This, some reflected, might form the basis of a feasible, dynamic and proactive approach, some form of multi-agency 'alert' or 'warning' system and 'round table' response:

'…if we think practically…how much can we do, I think it is far more around…where we sit within that space, sharing information, coming together to discuss…those concerns…seeing…those trends, those themes, those new and emerging things, because I think that's what we then respond to, isn't it?' (**Interviewee 9**)

While they felt that their communication and joined-up approach in these instances had been strong, what was missing was the detailed knowledge of how harm manifests online:

'…what we don't have is that understanding of exactly what online threats or exploitation looks like…all the different possible harms, all the different routes from perpetrators, all of those different exploitation tools that exist in that space and that space only. Yeah, we don't have enough information.' (**Interviewee 11**)

Academics and researchers, two respondents suggested, might have a role to play in informing a more evidence-based approach, feeding into training and toolkits for practitioners (who could then train others) because 'stuff is running at such a pace' (Interviewee 10) and 'people are really interested in it' (Interviewee 7). While these academics and other types of 'specialists' (in AI, data science) were important, they had to collaborate with child safeguarding experts to be effective. This was necessary but 'a hard bridge to cross' with these two groups having different priorities, levels of understanding and knowledge, 'trying to solve problems' together (Interviewee 11).

Finally, respondents were clear that 'trusted adults', including youth workers, guardians and mentors, were essential for safeguarding children from recruitment into CCE online: **'All a child needs is one trusted person they can speak to…'** (Interviewee 8). One member of the PEC's LEAP spoke in Session 1 (25 February 2026) about the importance of such 'trusted adults' also being online, going to where children 'are' and supporting them with the problems faced in that space as well as 'offline'. In relation to CSE online, CEOP has experienced Child Protection Advisers available online, alongside Childline, responding to reports submitted of online child sexual abuse.[3]

The Children's Society (2024) notes that youth workers and mentors provide an essential support role for children affected by CCE, enabling relationships with other professionals through advocating on their behalf. One respondent in our research spoke about this important relational role, taking time to 'build that positive relationship' with a child so that you learn what is 'actually going on' for them, things 'probably no one really knew before' (Interviewee 4). Another saw this as fundamental to mitigation of online recruitment and harm:

'…the basics…probably always been those protective factors…having activities for young people to do…things that they get involved in…that pull them away from those online spaces and ground them in something that's actually real, that gives them those trusted adults and people to talk to…I think those are probably going to remain some of your strongest interventions.' (**Interviewee 11**)

What comes through here is that good practice exists in terms of collaboration between frontline practitioners to address CCE online as well as a reaffirmation of the importance for children of 'trusted adults', information, digital literacy, support, activities and opportunities for prevention. There is also the suggestion of a more coordinated, deliberate effort or central mechanism where practitioners, working with other actors and experts, including those with digital technology expertise, can identify and respond quickly in real time to online recruitment as it expands, shifts, diversifies and evolves.

A child rights, child-centred approach

Our respondents were clear that 'championing the voice of the child' and understanding children's experiences (Interviewee 4) was essential for effective mitigation of online recruitment into CCE, but that children's expertise was frequently overlooked: **'...so often we see that young people's voices are forgotten about in this space and...it's really important that we remember that...it's them that this is happening to...'** (Interviewee 1).

The Children's Society (2024) notes that engagement of these children must be sophisticated, nuanced and trauma informed. One research respondent stressed some of the risks involved: **'...they're so petrified to engage, and...so scared to tell somebody because of the fear of repercussions that they have placed on them'** (Interviewee 4).

The NSPCC advocates for a child rights-based and child-centred approach to ensuring the 'safety-by-design' of digital platforms, apps and features, which it considers the most effective way to protect children from online harm: **'Technology companies must give due consideration to the rights and needs of child users, and design digital products accordingly'** (2025b:9).

Taking this further, the NSPCC has undertaken 'abusability testing' of ten digital 'services' used by children (names of platforms undisclosed) to assess the degree to which they can be abused to cause harm to girls. The study maps out a fictional girl's 'typical' user journey in setting up an online account for and using each 'service' and the potential of the design features she encounters to cause her harm. It finds that the responsibility to resist platform invitations to share her information and to reject approaches from strangers is placed almost entirely on the girl (NSPCC, 2025: 9-11).

Elsewhere, the NSPCC considers different models and mechanisms for 'putting children's voices at the heart of online safety regulation' (NSPCC, 2024a:5). They recommend that Ofcom has access to **'consistent, robust and unbiased evidence from children and safeguarding experts to build an agile understanding of harm and of new and fast-moving issues.'** This refers, in part, back to the importance of frontline practitioner knowledge and a coordinated response already mentioned above and the need to connect this up to those with digital expertise. The NSPCC goes on to recommend Ofcom ensures that **'there is an entity with a designated**

advocacy role for children's online safety,' addressing a major gap in the sector and **'risk that advocacy for children's safety online is happening in an ad-hoc way, rather than systematically and throughout Ofcom's decision-making process.'** Organisations like Barnardo's, The Children's Society and Action for Children are well-placed to support on feeding in children's lived experiences of recruitment into CCE online. The interconnections of any such a mechanism with existing and emergent entities focused on child safeguarding against exploitation would, however, be key since the online and offline worlds of children and their exploitation deeply intersect.

A fundamental component of any child-centred approach would require the recognition of children affected by online recruitment into CCE *as children*. Two respondents in our research spoke about the lack of participation and protection for children affected by child criminal exploitation, including online, because of how differently these children and child criminal exploitation are 'seen'. These practitioners argued against the criminalisation of these children and the tendency to 'victim-blame', which focuses on the criminal activity and offences committed by the child rather than the perpetrator - **'a child wouldn't be harmed if a perpetrator wasn't choosing to do so'** (Interviewee 1). This lack of focus also overlooks the exploitation of the child more generally:

'...people see criminal exploitation victims very differently...from sexual exploitation victims...these young people are engaged in criminal activity (coerced into doing so) so sometimes people lack the sympathy and understanding for that...it's really criminalising them. And we've had some really sad personal cases that we've had to work with, you know, with stabbings and all sorts of things. And, you know, all the talk in the media is about... 'lock that kid up!'...but no one's...thinking about the bigger picture of where that's come from...why has that young person ended up committing that offence...'
(**Interviewee 12**)

As previously suggested in this report - without in any way minimising or reducing our attention on other forms of child exploitation - we need to reflect further on why children who have been criminally exploited online remain relatively 'unseen' and make an urgent and concerted effort to address this. A child rights-based and child-centred approach is essential.

Adoption, adaptation, innovation

While participants in our research struggled to identify mitigations at a digital platform level for online recruitment into CCE, some drew on approaches related to other forms of child exploitation, for example CSE, or child safety online more generally, considering how these might be adopted or adapted. One of these approaches was based on Swansea University's DRAGON programme.

DRAGON (Developing Resistance Against Grooming Online)[4] is a digital innovation programme hosting a portfolio of research projects using expertise in communication to improve crime prevention and child protection efforts, with a focus on CSE and abuse. The programme is focused on how grooming uses

language to build trust, isolate children and escalate harm and draws on cutting-edge research and technology from across the social and computer sciences, including linguistics, to develop strategies to safeguard children and disrupt exploitation and abuse. Two significant and complementary initiatives operate as part of the programme: DRAGON-SHIELD, an interactive, multimedia training course that helps users understand how groomers and children communicate during online grooming conversations. The other, DRAGON-SPOTTER, was created to support law enforcement through improving how to spot and respond to grooming online. Importantly, and referring back to the importance of collaboration, child participation and an ecosystem of actors above, DRAGON has co-creation at its centre, working with key stakeholders (child safeguarding practitioners, children, lived experience experts, researchers) as well as organisations across Wales, the UK and internationally to address grooming into CSEA online.

Two of our respondents saw potential for the DRAGON programme to address CCE online, one suggesting its adaptation and roll-out at scale:

'…you are starting to see some programmes…like DRAGON…I know that's specifically…for…online grooming…but…I've said already…how…sexual exploitation grooming looks…very similar sometimes to…criminal exploitation…So, I think if you used…that on a really wide scale…you could be intercepting these communications. If…tech companies…really took on board this type of programme and software you could…at least do a better job than is currently done…because it needs to be…information based…it is actually based on a grooming pattern and…flagging…at the point of grooming by identifying that's a concerning…conversation…give that to…the tech provider, contacts, local police force… something like that DRAGON software could be used as a…prevention kind of system.' (**Interviewee 3**)

The other respondent focused on school safeguarding alert systems and how these might be adapted and informed by DRAGON's approach:

'I was thinking about another mechanism…and this is going back to…in schools…you've got your MyConcern which allows practitioners to log straight away any concerns that need to go to safeguarding. And then other companies have then brought in additional elements to that. And some of them are installed as an IT package in the school. And…there will be certain words that are then flagged up so what you get when you log on is obviously all of the children that are linked comments, and then you can look and see what they've been looking at or where they've been…So I guess what is probably under development…is ways of picking out data in the way that SHIELD are doing…but trying to find those key elements or words or something like that that would help you identify where young people are at risk.' (**Interviewee 11**)

In addition to this substantive initiative, one practitioner interviewed was able to speak about emerging practices tackling CCE online, for example the police producing 'counter' adverts **'that look like the ones that a child would click on and maybe be exploited'** but then provides **'an outline of what exploitation can look like'** (Interviewee 5) and alerts and educates them.

Whilst no academic publications focused on mitigating CCE online were identified through our literature review, a whole body of published research explores the mitigation of child sexual exploitation online. For example, a similar initiative to the police 'counter' adverts was explored by Scanlan et al. The study focused on access to online child exploitation materials (CEM) and suggested that 'honeypot' websites might be set up as a 'lure for bad actors', enabling their identification and facilitating warning messages 'to educate within that situation, to change behaviour' and 'to prevent the crime from occurring' (2021:6). Alternatively, Urbas (2021) explores the adoption of AI in the investigation of online child sexual exploitation, taking as a case study the development of an autonomous childlike avatar called 'Sweetie 2.0' used by NGO Terre des Hommes to identify webcam-based child sexual predators. Other initiatives set up by NGOs are reported on in the 'grey literature'. For example, the NSPCC and Childline are collaborating with the Internet Watch Foundation (IWF) on 'Report Remove',[5] an initiative supporting children to safely and confidentially report sexual images or videos of themselves that have been shared online and removing these from the internet. Given the findings from this research on criminally motivated child sexual extortion and the interconnections between CSE and CCE, this initiative has relevance.

While the research did not identify tailored interventions addressing online recruitment of children into CCE, this does not mean that new or emerging mitigations do not exist or cannot be co-designed, nor that we should overlook pre-existing solutions generated to address online recruitment into other forms of child exploitation. It is imperative to investigate what other evidence-informed initiatives exist that tackle CSE online, with transferable potential and/or learning for the purpose of disrupting online recruitment.

[1] A social media ban for under-16s has been announced by the UK government. It will be introduced in early 2027.
[2] https://online-risk-guide.barnardos.org.uk/
[3] CEOP Safety Centre
[4] Home - DRAGON Developing Resistance Against Grooming Online
[5] Report Remove from Childline and IWF

7: Conclusions

This research report has explored and sought to understand the online recruitment of children into criminal exploitation (CCE) in the UK. It has identified a significant and concerning gap between the level of harm happening to children and the attention given to this issue in the academic literature and beyond.

We believe that this has been the first dedicated research project to investigate CCE in the UK as it manifests online: the digital platforms involved, the children at risk, the recruitment pathways and tactics employed, the harms to children that result and potential mitigating interventions. It also, in the accompanying 'gap analysis', investigates how online recruitment into CCE fits within current UK legal definitions, law, policy and guidance frameworks, as well as the implications for how online harm is prevented, how children are identified and protected and how perpetrators can be disrupted and prosecuted.

This substantive focus on online recruitment into CCE in the UK is long overdue. It is clear that organised criminal groups, their networks and activities, significantly shifted online during the COVID-19 pandemic; and that related lockdowns and have remained 'hybrid' ever since, exploiting children both online and 'offline' at an ever-increasing scale. UK children's charities working to address CCE, like The Children's Society, Action for Children and Barnardo's, reported on this concerning issue in real time, campaigning for its explicit inclusion in the UK Online Safety Act (OSA) alongside the attention given to online child sexual exploitation (CSE). They had recognised and highlighted the intersectionality of these and other forms of child exploitation and warned against a 'siloed' approach. However, the OSA does not yet include CCE as an online risk to children alongside CSE and this needs to be addressed as a matter of importance.

The process of conducting this research has been marked by contrast. On the one hand, the academic literature tells us very little about how CCE in the UK manifests online. This topic is given brief attention and positioned mostly on the margins of CCE research. On the other hand, interviews with practitioners addressing CCE online are clear that this is complex, dynamic, happening across multiple digital platforms and at scale. While certain platforms and risks can be identified, they stress that such recruitment can potentially take place on 'any platform' and affect 'any child'. They also emphasise the complex and evolving nature of the problem where recruitment pathways adapt, shift and change. Practitioners feel overwhelmed and under-equipped in their efforts to prevent and disrupt such exploitation.

A further area of misalignment is the deep harm caused by the online recruitment of children into criminal exploitation and its underestimation. Interviewees and NGO reports document in detail the all too real harms experienced by those children affected and contest the perception that harm is minimal where this takes place 'just' or 'only' online. It is also clear that multiple, intersecting forms of harm – physical, sexual, emotional, psychological, financial, criminal – can and do occur as the exploitation evolves. Criminalisation and 'victim blaming' are preventing the protection of these children and a significant reconceptualization of these children whose rights are being abused.

Despite this catalogue of harm, limited interventions and mitigations targeting online recruitment of children into criminal exploitation are identified through this research. A lack of data and academic investigation are an obstacle to addressing this problem and to designing effective interventions. There is potential to learn from effective existing interventions, for example those addressing grooming and CSE online (where much academic research and digital expertise have focused), if we recognise the intersectionality of exploitation and the commonalities in the grooming/recruitment process. There is also potential for innovation, bringing safeguarding and digital experts together with children affected by online recruitment to generate feasible and agile solutions that respect children's rights and needs and can operate effectively at scale. Such mitigation requires a system-wide response, building on efforts to address all forms of child exploitation both online and 'offline' in recognition of the deep interconnections and intersectionality that exists.



8: Recommendations

This research demonstrates that children at risk of and affected by online recruitment into criminal exploitation remain relatively unseen and require our urgent attention. The following recommendations related to law, policy and practice as well as awareness-raising are intended to address this and achieve a significant shift in the visibility and protection of these children.

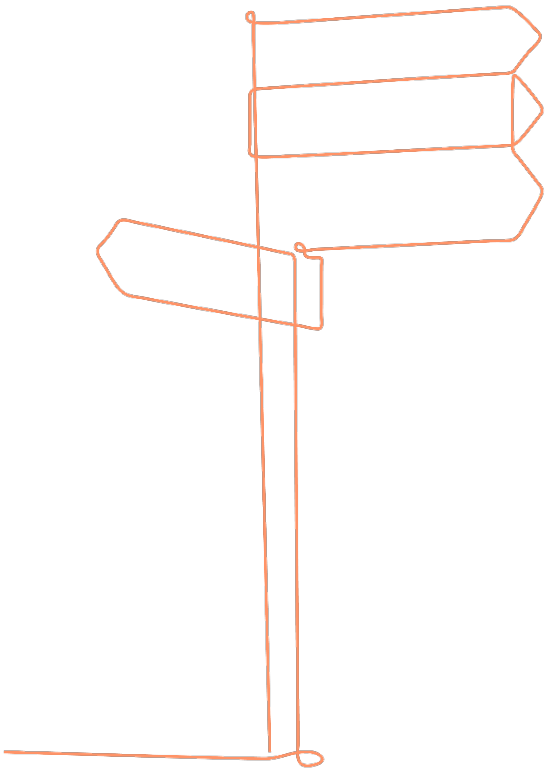
- **Recommendation 1:** The UK government should make CCE a priority offence under the Online Safety Act (OSA) by including it in Schedule 7 of the Act. This new CCE priority offence should not be siloed but considered alongside other priority offences, existing and future, relating to child exploitation and human trafficking as well as harmonised with the 2026 Crime and Policing Act definition of CCE. Statutory guidance on CSEA harms should explicitly recognize how child sexual exploitation (CSE) and intimate image abuse can be criminally motivated and intersect with CCE.

- **Recommendation 2:** Ofcom should address CCE in the Children's Code of Practice and include it in the Children's Register of Risks as an additional risk. The new entry in the Children's Register of Risks should recognize the interconnection of CCE with multiple other risks, harms and offences that 'victims' of CCE can encounter, such as, but not limited to, grooming, intimate image abuse, and coercive and controlling behaviour.[1] CCE should also be recognized in Ofcom's general online safety Register of Risk.

- **Recommendation 3:** The forthcoming MoJ Statutory Guidance on the Crime and Policing Act 2026 must recognize online recruitment into Child Criminal Exploitation (CCE) and CCE as manifest online in its formal definition of CCE. The Guidance should raise awareness of the potential risks to children of being recruited online into criminal exploitation, the methods employed by perpetrators and the harms involved. The interconnection between online and 'offline' tactics and harms as well as between CCE and CSE and other forms of child exploitation and human trafficking must be highlighted.

- **Recommendation 4:** The IASC working with the Department of Education, Home Office and devolved equivalents should raise awareness of all 'first responders', guardians and trusted adults on - and drive integration of - the online recruitment of children into criminal exploitation into multi-agency, child-centred efforts to safeguard children from exploitation. Such collaborations should include the ongoing identification of gaps in knowledge and safeguarding practices related to online recruitment, as well as the development of tools, resources and mechanisms needed by frontline practitioners for support.

These recommendations should be read and considered in conjunction with the broader, system-level recommendations addressing the exploitation of children in the accompanying Gap Analysis report.



9: References

Barnardo's (2021) Exploited and criminalised: What can the Police, Crime, Sentencing and Courts Bill do to ensure that children who are criminally exploited receive the care and support they need?

Barnardo's (2023) Knife Crime General Debate: Monday 16 October, 2023.

Barnardo's (2023a) Barnardo's briefing paper June 2023: Child exploitation: A hidden crisis.

Barnardo's (2023b) Invisible children: Understanding the risk of the cost-of-living crisis and school holidays on child sexual and criminal exploitation.

Barlow, C., Kidd, A., Green, S.T. and Darby, B. (2022) 'Circles of analysis: A systemic model of child criminal exploitation', Journal of Children's Services, 17(3), pp. 158-174.

Counter Terrorism Policing, NCA and NPCC. 2026. 'Com Networks: Alert for Safeguarding Children Partnerships'.

Dixon, N. (2023) Understanding child criminal exploitation in Scotland: A scoping review. Glasgow: Children and Young People's Centre for Justice (CYCJ). Available at: https://www.cycj.org.uk/wp-content/uploads/2023/05/Understanding-Child-Criminal-Exploitation-in-Scotland.pdf (Accessed: [date]).

Duddy, C. and Wong, G. (2023) 'Grand rounds in methodology: When are realist reviews useful, and what does a "good" realist review look like?', BMJ Quality & Safety, 32(3), pp. 173-180.

Firmin, C. (2017) Abuse Between Young People: A Contextual Account. 1st edn. London: Routledge.

Firmin, C. (2020) Contextual safeguarding and child protection: Rewriting the rules. London: Routledge.

Firmin, C. (2024) 'Binaries and blurred lines: The ethical stress of child protection social work in the grey of extra-familial harm', Ethics and Social Welfare, 18(4), pp. 404-421

Firmin, C. (2026) 'Daring to Care: Seeking ethical social work with children and young people', The British Journal of Social Work, 56(3), pp. 797-804.

Firmin, C., Lefevre, M., Huegler, N. and Peace, D. (2022) 'Safeguarding young people beyond the family home: Responding to extra-familial risks and harms', in Safeguarding Young People Beyond the Family Home. Bristol: Policy Press

Firmin, C., Lefevre, M., Langhoff, K. and Ruch, G. (2025) 'A line in the sand: Moving from surface improvement to foundational shifts to develop effective responses to extra-familial risks and harms', The British Journal of Social Work, 55(3), pp. 1296-1316.

Firmin, C. and Lloyd, J. (2017) Contextual safeguarding: An overview of the operational, strategic and conceptual framework. Luton: University of Bedfordshire.

Firmin, C. and Lloyd, J. (2022) 'Green lights and red flags: The (im)possibilities of contextual safeguarding responses to extra-familial harm in the UK', Social Sciences, 11(7), p. 303.

Firmin, C., Lloyd, J. and Bernard, C. (2023) Contextual Safeguarding. Bristol: Bristol University Press

Firmin, C., Manister, M. and Peace, D. (2023) 'Serious case reviews and extra-familial harm: Missed and emerging opportunities to develop contextual practices', The British Journal of Social Work, 53(2), pp. 1077–1098.

Firmin, C., Peace, D. and Wroe, L. (2026) 'Why "common sense" is complicated: Unearthing the cultural facilitators of contextual safeguarding structures', Journal of Social Work

Kane, G., and Chisholm, A. (2025) Identifying modern slavery and human trafficking in the context of child criminal exploitation in Northern Ireland.

Larasati, A. and Wahyudi, S.T. (n.d.) 'Criminal policy on prevention of child exploitation in the form of donation requests through the TikTok platform', Law Development Journal, 6(4), pp. 503–513.

Maxwell, N. (2023) 'I'm trying to save my family: Parent experiences of child criminal exploitation', Youth Justice, 23(2), pp. 243–258.

Maxwell, N. (2026) '"Shove that. There's always hope": Young people's lived experience of child criminal exploitation', Journal of Youth Studies, 29(1), pp. 54–70. Available at: https://doi.org/10.1080/13676261.2024.2397025

Maxwell, N. and Corliss, C. (2024) '"I am not going to lie; some people do not even want to talk": Co-design with vulnerable groups affected by child criminal exploitation', Children & Society, 38, pp. 1692–1713. Available at: https://doi.org/10.1111/chso.12833

Maxwell, N., Wallace, C., Cummings, A., Bayfield, H. and Morgan, H. (2019) A systematic map and synthesis review of child criminal exploitation.

Maxwell, N. and Wallace, C. (2021) Child criminal exploitation in Wales.

McLean, R., Robinson, G. and Densley, J.A., 2019. County Lines: Criminal Networks and. Evolving Drug Markets in Britain. 1st edition, Cham: Springer.

NSPCC (2023) Evidence review on online risks to children.

NSPCC (2025) Targeting girls online: How online services enable the abuse and harassment of girls

NSPCC (2025) Viewing generative AI and children's safety in the round.

Palmer, T. (2015) Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people. Barnardo's and The Marie Collins Foundation.

Pawson, R., Greenhalgh, T., Harvey, G. and Walshe, K. (2005) 'Realist review: A new method of systematic review designed for complex policy interventions', Journal of Health Services Research & Policy, 10(Suppl. 1), pp. 21–34

Robinson, G., 2020. Gangs, county lines and child criminal exploitation: a case study of Merseyside. Edge Hill University (United Kingdom).

Saul, J.E., Willis, C.D., Bitz, J. and Best, A. (2013) 'A time-responsive tool for informing policy making: Rapid realist review', Implementation Science, 8(1), p. 103.

Scanlan, J., Watters, P.A., Prichard, J., Hunn, C., Spiranovic, C. and Wortley, R. (2022) 'Creating honeypots to prevent online child exploitation', Future Internet, 14(4), p. 121. Available at: https://doi.org/10.3390/fi14040121

Sheehan, K., Walsh, C. and Cusack, A. (2024) '"It's a group-on-one": Social disconnection as a tool of and defence against child criminal exploitation in the Republic of Ireland', Crime Prevention and Community Safety, 26(3), pp. 266–284.

Stott, H. (Forthcoming 2026) Understanding online recruitment of children into criminal exploitation in the United Kingdom: Gap analysis. Modern Slavery PEC.

The Centre for Social Justice and Justice & Care (2024) Criminal exploitation: Modern slavery by another name.

The Children's Society (2019) Counting lives: Responding to children who are criminally exploited.

The Children's Society (2024) Online Safety Act: Protecting children from harms online consultation – The Children's Society response.

The Children's Society (2024) What do we mean by "child criminal exploitation"? The need for a clear rights-based legal definition.

The Children's Society (2025a) Moving money: Uncovering the reality of exploitative money laundering and other forms of child financial exploitation.

The Children's Society (2025b) Tackling financial exploitation: Youth voice insights.

UK Government (2023) Criminal exploitation of children and vulnerable adults: County lines guidance. 20 October.

UK Government (2024) Money laundering-linked financial exploitation: Guidance for frontline professionals (accessible). Policy paper. 1 March.

UK Government (2026) Modern slavery: National Referral Mechanism and Duty to Notify statistics UK, end of year summary 2025. Official statistics. 19 February.

Urbas, G., 2021. Legal considerations in the use of artificial intelligence in the investigation of online child exploitation. ANU College of Law Research Paper, (21.44).

Walsh, C. (2023) 'From contextual to criminal harms: Young people's understanding and experiences of the violence of criminal exploitation', Crime Prevention and Community Safety, 25(3), pp. 282–304

Wroe, L.E., Peace, D. and Firmin, C. (2023) '"Relocating" adolescents from risk beyond the home: What do we learn when we ask about safety?', The British Journal of Social Work, 53(5), pp. 2958–2978.

MODERN SLAVERY & HUMAN RIGHTS | POLICY & EVIDENCE CENTRE

Led by the University of Oxford

The Modern Slavery and Human Rights Policy and Evidence Centre (the PEC) at the University of Oxford exists to enhance understanding of modern slavery and transform the effectiveness of laws and policies designed to address it.

The Centre funds and co-produces high quality research with a focus on policy impact, and brings together academics, policymakers, businesses, civil society and survivors to collaborate on solving this global challenge.

The Centre is a consortium of three Universities of Oxford, Liverpool and Hull, and is funded by the Arts and Humanities Research Council (AHRC) on behalf of UK Research and Innovation (UKRI).

pec.office@humanities.ox.ac.uk
www.modernslaverypec.org

Authors: Dr Anna Skeels, SPARK, Cardiff University

Published by: Modern Slavery and Human Rights Policy and Evidence Centre, University of Oxford.

Publication date: November 2026

©2026, Dr Anna Skeels.

This work is openly licensed under a Creative Commons Attribution 4.0 International Licence CC BY 4.0.

This work was supported by the Modern Slavery and Human Rights Policy and Evidence Centre, University of Oxford [reference number: R90817/CN001] from its grant from the Arts and Humanities Research Council [grant number AH/T012412/2].

Identification number of the publication: PEC/2026/16

Our partners:

University of Hull | Wilberforce Institute

University of Liverpool

Bonavero Institute of Human Rights

BICL British Institute of International and Comparative Law

Funded by:

UKRI Arts and Humanities Research Council