LSCP Multiagency Practice Guidance
Online Safety

December 2025

This Guidance is owned by Lambeth Safeguarding Partnership (LSCP) for use by multi-agency staff working with children in Lambeth.

Contents

Version Control

Date issued	Version	Summary of changes	Created by	Approved by
09/12/2025	V1	Initial draft	G Russo	LSCP Executive Board

Intended audience
The Practice Guidance on Online Safety must be shared, for information purposes, with all managers and practitioners with safeguarding responsibilities across:

- Lambeth Council
- South East London Integrated Case Board
- Metropolitan Police Central South Basic Command Unit

1. Introduction

Technology has become an integral part of children and family life. It can offer many benefits, including opportunities for learning, education and social interaction. However, the online world is also a space where children can be at risk of, and experience, harm. Where children have complex and intersectional vulnerabilities, there is an increased risk to children online.

National research evidence shows that:

- Technology-facilitated abuse patterns in domestic abuse cases are frequently under-recognised, leaving children exposed to continued harm through digital means.
- Online connection-seeking behaviour by children who are looked after is often misinterpreted as "risky behaviour" rather than understood as meeting legitimate developmental needs.
- Children with mental health needs are drawn to harmful online content during periods of distress, but this is rarely factored into safety planning.

These patterns represent countless missed opportunities across our system to protect vulnerable children online.

The Local Child Safeguarding Practice Review for Olivia[1] highlighted the complex interplay where social media is both a source of comfort for children and a vehicle used to cause them harm. Olivia was a child who was looked after and neurodivergent. She experienced multiple instances of physical and sexual harm and social media was a contributing factor to the exploitation she experienced. Practitioners involved in the review highlighted the challenges experienced in trying to safeguard Olivia against this risk; with the review concluding there was a need for multiagency guidance to support practitioners around safe and effective engagement with social media when safeguarding children.

2. About this guidance

2.1 Aims and objectives

This guidance aims to increase practitioner confidence and ability to recognise and respond to the risks posed to the children in the online world. Specifically, it seeks to:

- Raise awareness of the nature and scope of online risks, including evolving harms such as AI-generated abuse, live streaming and targeted grooming.
- Support professionals in making confident, proportionate decisions when responding to online safety issues.
- Establish a consistent, multi-agency approach to identifying, preventing and responding to online safety concerns.

[1] Available on the NSPCC Repository here.

This guidance should be used:

- As guidance and a framework for supervision to explore complex cases.
- To inform comprehensive assessment that considers all risk factors.
- To guide multi-agency discussions about vulnerable children's online safety.
- To support trauma-informed practice adapted to different presentations.
- To build understanding of how different vulnerabilities manifest online.
- To identify and respond to digital neglect across all vulnerable groups.
- To develop coordinated safety plans that address intersecting needs.

2.2 Scope of guidance

This guidance is aimed at all practitioners working with children living in, or looked after by, Lambeth and/or working with their families.

2.3 Definitions

We use the term "**children"** to refer to all people under the age of 18.

We use the term "**practitioners**" to refer to all staff and volunteers working in agencies who have functions in relation to children or their families.

We use the term "**safeguarding**" to describe the measures and practices put in place to protect children from harm and as defined in Working Together to Safeguard Children.

We use the term "**online safety**" to describe the protection of individuals from harmful content, conduct, contact and commercial risk in digital environments, and the promotion of positive, responsible and informed online engagement. "**Digital harm**" describes any abuse, exploitation or psychological harm experienced via online platforms or digital interactions.

We use the term "**digital neglect**" to describe a failure to meet a child's online safety and wellbeing needs. This is increasingly recognised as a significant safeguarding concern that requires the same attention as other forms of neglect. This neglect disproportionately affects children with existing vulnerabilities, creating compounding risks that demand adapted responses.

We use the term "**neurodivergent**" to describe children whose brain functions, learns, and processes information differently than what is considered typical or "neurotypical". This encompasses a wide range of neurological differences, including conditions like Autism Spectrum Condition (ASC) and Attention Deficit Hyperactivity Disorder (ADHD).

We use the term "**trauma-informed**" to describe an approach that recognises and responds to the impact of traumatic experiences on behaviour and development; and

the term "**vulnerability-informed**" to describe approaches which are adapted to account for specific vulnerability factors and their intersections.

A full glossary of terms can be found in Appendix E.

2.4 Legal and policy framework

This guidance should be reach alongside:

- LSCP Online Safety Policy
- Lambeth's Multi-Agency Arrangements to Safeguard Children (December 2024)
- London Safeguarding Children Procedures
- London Threshold Document
- Working Together to Safeguard Children 2023
- Online Safety Act 2023
- Lambeth's Neglect Strategy and Neglect Toolkit

2.5 Key principles

This guidance is guided by the following core principles:

- **Safeguarding is everyone's responsibility - including online**. Practitioners have a duty to understand online risks and respond appropriately.
- **Equity and inclusion are essential**. Certain individuals and communities face greater risk online due to systemic barriers, unmet needs or interesting vulnerabilities. Online safety responses must be inclusive, accessible, trauma-informed and vulnerability-informed.
    - Every vulnerable child deserves an online safety approach adapted to their specific needs.
    - Multiple vulnerabilities require coordinated, not competing, responses.
    - Digital neglect is a safeguarding concern requiring active intervention.
    - Online spaces often meet legitimate needs for vulnerable children.
    - Punitive approaches to online behaviour often re-traumatise.
    - Responses must be therapeutic and supportive, not controlling.
- **Working together is vital**. No single agency can keep children safe online.
- **Safety and Empowerment Go Hand in Hand.** Online safety is not just about restriction and control. It's about building knowledge, confidence and autonomy, especially in children. A safeguarding approach that empowers users is more likely to be effective and sustainable.
- **Digital Opportunities Should Be Promoted.** While managing risks, we must also recognise and promote the positive aspects of digital technology, including education, creativity, connection and participation in modern society.
- **Think Family and Consider Context.** Professionals must consider the whole family in context when addressing online safety, recognising that digital harm often affects multiple family members and that solutions require a whole-family approach.

3. Understanding online risks

Online risks are diverse, evolving and often hidden. Children may experience harm through exposure to content, harmful interactions, their own behaviour online or the design of digital systems themselves. These risks may occur across social media, messaging apps, games, virtual learning environments and newer technologies such as AI-driven platforms or livestreaming. Children may use multiple devices to access the online world including smartphones, laptops, gaming consoles, tablets, desktop computers, smart devices (like TVs, watches and speakers) and 'Internet of Things' devices (like cameras and appliances able to connect online to provide remote control and automation).

Practitioners must be equipped to recognise and assess the nature, context and impact of these risks, especially when they may not be immediately visible or disclosed.

3.1 The 4Cs of online risk

Lambeth adopts the UK Council for Internet Safety (UKCIS) model of the 4 Cs, which categorises online risks into four interlinked areas:

Content Risk What the user sees or is exposed to:

Harmful or inappropriate content including:

- Pornographic, violent or disturbing visual content
- Pro-suicide, self-harm or eating disorder material
- Hate speech or extremist/terrorist propaganda
- Content that promotes hatred or discrimination based on race, gender, sexual orientation, gender identity or other protected characteristics.
- Medical misinformation or conspiracy theories.
- Content that deliberately targets and exploits specific groups who may face particular vulnerabilities online.
- Algorithmic exposure to harmful trends (e.g. TikTok "challenges").

Contact Risk Who the user interacts with:

- Online grooming or coercive contact by adults or peers.
- Sexual exploitation involving threats, coercion or blackmail (including 'sextortion').
- Exploitation through livestreaming or webcam use.
- Recruitment into gangs, extremist groups, cults or cult-like movements.
- Online radicalisation or exposure to incel, Extremist Right Wing (XRW) and Islamist ideologies.
- Manipulative peer networks or online "friendships" used to isolate individuals.
- Technology-facilitated domestic abuse.

Conduct Risk How the user behaves online:

- Cyberbullying or online harassment.
- Sharing nudes or semi-nudes (self-generated sexual imagery, also know as 'sexting').
- Engaging in abusive or exploitative behaviour towards others.
- Creating or sharing extremist/terrorist material (a key indicator for Prevent).
- Posting risky or personal content (oversharing).
- Participating in harmful trends or dares.
- Digital disinhibition: behaving in ways online that they would not offline.

Commerce risk Risks related to money and personal data:

- In-app purchases or gambling-like features in games.
- Online scams, phishing or financial exploitation.
- Exposure to hidden advertising and influencer marketing.
- Sale of personal data or manipulation through targeted ads.
- Crypto scams or unregulated digital transactions.

3.2 Emerging and Evolving Risks

Online harm is consistently shifting in form and platform. Professionals must stay informed about:

- AI-generated abuse: deepfake pornography, cloned voices and manipulated images.
- Digital self-harm: posting abusive or negative messages about themselves anonymously and/or deliberately seeking out content that is likely to cause them distress.
- Livestreaming platforms: increased risk of coercion, impulsive behaviour or abuse.
- Anonymous messaging apps: used for bullying, grooming or emotional manipulation.
- Online "communities": that glamourise eating disorders, self-harm, hate ideologies or anti-help narratives.
- Online platforms used for emotional release and validation: these can be both protective and risky.
- Augmented reality and metaverse spaces: emerging risks around digital identity, exploitation and regulation gaps.
- Cross-border exploitation: where perpetrators operate from outside UK jurisdiction.

4. Vulnerability factors

All children can experience harm online and practitioners must be able to recognise and respond to indicators of online harm for all children.

However, certain children are considered more vulnerable to online risk. Online spaces serve both as a sanctuary and a risk for vulnerable children. Understanding this duality is crucial for developing effective responses that protect without unnecessarily restricting beneficial connections.

Practitioners should recognise that when children connect to the online world they are seeking to fulfil a need. Effective responses should always seek to understand what needs are being met online that aren't met offline.

4.1 Vulnerable groups

This guidance recognises that specific vulnerability factors increase online risk and that it is important to recognise how vulnerabilities interact to create compound risks. Practitioners should adapt standard approaches to match children's specific needs and presentations.

This guidance provides specific frameworks for:

- Children who are looked after who may seek connection online and have less family protection.
- Neurodivergent children whose traits may increase online vulnerability.
- Children affected by domestic abuse who face technology-facilitated harm.
- Children with mental health needs who may be drawn to harmful online content.
- Children experiencing poverty who face digital exclusion and unsafe access.
- Children with communication needs who face accessibility barriers.
- Children who have been criminally and sexually exploited.

4.2 Understanding the push factors

Vulnerable children may see the online world as a place of sanctuary and comfort. Their vulnerability can 'push' the child towards the online world and create an increased risk of harm. For example:

Neurodivergent children	Studies show that for neurodivergent children, online spaces often represent their primary social world. Cutting them off can increase isolation and mental health difficulties.

Children who are looked after	Online spaces often serve as primary social connection for children in care, providing belonging and identity exploration that may be disrupted by placement moves and being far away from friends and family networks. However, this same connection-seeking can expose them to exploitation by adults who target their vulnerabilities.
Children affected by domestic abuse	Technology provides escape and support for children experiencing domestic abuse, offering access to help services and safe social connections. Yet perpetrators increasingly use the same platforms for surveillance, control and continued abuse. Children in these situations face both direct and digital abuse and exposure to technology-facilitated abuse between adults.
Children with mental health needs	Online communities can provide vital peer support and understanding for children with mental health difficulties, reducing isolation and shame. However, algorithms can also amplify harmful content during vulnerable periods, leading to communities that promote self-harm or eating disorders. The Online Safety Act 2023 specifically addresses platforms' duties regarding mental health content, recognising the particular vulnerabilities of children accessing pro-suicide and self-harm content.
Children experiencing poverty	Online spaces provide essential access to education, social service and support networks for children facing financial hardship. However, poverty often means a lack of access – so a child having to use library computers after school may be unable to access help safely due to time limits and lack of privacy, while another child sharing a phone with siblings may find their conversations monitored by family members. Children can further be reliant on cheaper platforms with fewer safety features.

Children with communication needs	Digital platforms can provide crucial accessibility features and communities for children with communication difficulties – visual communication tools, translation services, and peer support networks. Yet these same children may struggle to understand safety warnings, report concerns or access help due to language barriers or communication difficulties.
Children who have been criminally and sexually exploited	Online spaces can provide opportunities to escape reality and provide distraction and relief from trauma, as well as potential for emotional reassurance and validation. Yet these same children may normalise and struggle to recognise online exploitation and may find abusers seeking to control them through technology.

4.3 Intersectional vulnerability

Children rarely present with single vulnerabilities. For example, a child may be looked after, neurodivergent and experiencing mental health difficulties. These intersecting vulnerabilities create unique online risk profiles that cannot be addressed through generic approaches.

Effective safeguarding responses must explore vulnerability factors through an intersectional lens. Consider these examples of intersecting vulnerability:

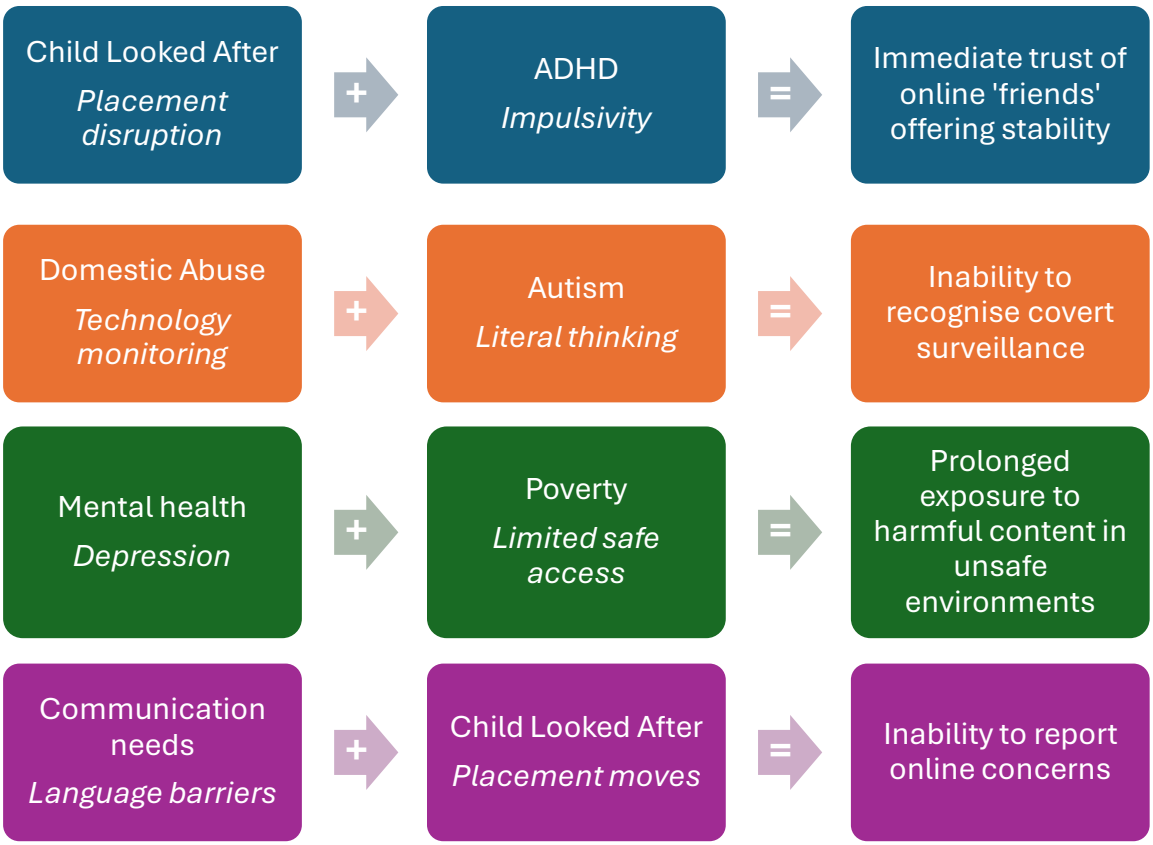
- *Child Looked After + Mental Health*: A child in care with depression may seek validation online, making them vulnerable to grooming while also needing the connection for emotional survival.
- *Domestic Abuse + Poverty*: A child from a family experiencing domestic abuse and financial hardship may only have access to unsafe public Wi-Fi, making them vulnerable to monitoring while also needing online access for safety planning.
- *Neurodivergent + Communication Needs*: An autistic child whose first language is not English may struggle to understand safety information due to both factors, making them vulnerable to exploitation, while their family may not understand risks or understand advice available in English.
- *Mental Health + Poverty*: A child with anxiety who relies on shared devices may be unable to seek help safely online, increasing isolation and mental health risks.

Children's vulnerability can be amplified by associated amplifying factors. For example:

- Social isolation
- Placement instability
- Family circumstances

- Trauma history
- Cultural factors
- Educational disruption

When vulnerabilities combine, they don't simply add together, they can create entirely different risk profiles. For example:



Practitioners must consider all of children's vulnerabilities through an intersectional lens in order to understand specific online risks and respond in a vulnerability-informed manner.

5. Recognising signs of online harm

Online safety concerns may present in several ways, including:

- A child discloses something directly.
- Concerning content, messages or behaviours are observed by professionals.
- A parent or carer raises a concern.
- A safeguarding incident involves digital devices or platforms.
- A pattern of behaviour or distress is linked to online activity.
- Digital neglect is identified.
- Technology-facilitated domestic abuse is suspected.

Other signs that a child may be experiencing online harm include (but are not limited to):

- Secretive or obsessive use of devices.
- Emotional distress after going online.
- Withdrawal from offline relationships or activities.
- Rapid changes in mood, sleep or self-esteem.
- Talking about new online "friends".
- Rapidly changing online connections that are difficult to track or map.
- Using multiple online identities or accounts.
- Unexplained financial activity or possessions.
- Knowledge of sexual or violent content that is inappropriate for their age.
- Sudden changes in views or beliefs influenced by online sources. This can include, but is not limited to:
  - Changes in views and beliefs due to bullying, harassment, online relationships, or a need to find escape from situations in their everyday life.
  - Changes in views or beliefs due to accessing or being sent extremist/terrorist online content, which would be a Prevent concern.
- Physical symptoms (headaches, sleep disturbance) linked to screen use.
- Reluctance to discuss online activities or defensive behaviour.
- Not attending virtual appointments or online sessions.

Practitioners should be especially alert to disclosures or cues about digital harm during assessments, conversations or family support work, even when the issue is not raised directly.

Digital neglect should be considered alongside other forms of neglect and where identified practitioners should use the LSCP's Neglect Toolkit to inform their responses.

6. Assessing online risk

Whether concerns about online risk arise from an incident, a disclosure or observation, there is a need to assess the level of risk alongside any contributing vulnerability factors to inform effective responses.

Assessments must include consideration of:

- How do their specific vulnerabilities manifest online?
- How do these vulnerabilities interact to create particular safety needs?
- What needs are being met online that aren't met offline?
- How do they process online information differently due to their vulnerabilities?

A key principle of assessment is that each vulnerability requires adapted approaches, and combinations require coordinated multi-agency responses that address thew hole child, not competing single-issue interventions. This is **vulnerability-informed** practice.

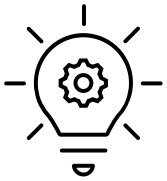
When online harm is suspected or disclosed, practitioners must consider:

- What type of risk is present? (e.g. grooming, exposure, conduct, obsessive interest in conspiracy theories)
- How is it affecting the child's wellbeing, behaviour or relationships?
- What is the balance between digital restriction for safety versus the child's mental health and connection needs?
- Is there a wider safeguarding concern, such as exploitation or coercion?
- Are there others at risk? (e.g. siblings, peers, online contacts)?
- What protective factors are present, and what support is needed?
- Are there cross-border or jurisdictional complications?
- Is this linked to other forms of harm (e.g. neglect, domestic abuse)?

The Online Safety Risk Assessment Template provides an assessment framework to consider these factors. This should be used when:

- Online safety risks are suspected or disclosed during any professional contact.
- Virtual non-attendance raises safeguarding concerns.
- Multiple vulnerability factors are present that increase online risk.
- Multi-agency coordination is required to address digital harm.
- Developing digital safety plans or interventions.
- Reviewing and updating existing safeguarding plans to include online safety considerations.

Risk assessments need to be done in collaboration with children, their families and their multiagency networks. Practitioners should recognise that children can be wary and secretive about their online world and may view direct questions about social media use as intrusive.



Top Tip! *why not try a playful and curious approach? Ask the child to show you how to play the game they are most into or show you some of their favourite TikTok videos. Use this as an opportunity to explore more, for example, who they interact with and how often they interact with the platform. What other platforms do they use? Encourage parents & carers to adopt the same approach!*

Effective risk assessments must also be informed by understanding of specific vulnerabilities. Section 7 provides detailed guidance for understanding and responding to online safety concerns for children with specific vulnerabilities (whilst recognising the unique ways that different vulnerabilities manifest in online environments).

7. Responding to online risk

The level of response to online risk should always be informed by the London Threshold Document. Some online concerns additionally require tailored responses.

Practitioners should refer to specialist guidance or seek advice in the following situations:

- **Self-Generated Sexual Imagery**
  - Follow guidance in UKCIS: Sharing Nudes And Semi-Nudes.
  - Do not view or share the images.
  - Report to your safeguarding lead/manager (or make a direct referral if you are an experienced professional in health settings) and determine if police involvement is required.
  - Address the underlying safeguarding needs of all involved.
  - Consider restorative approaches where appropriate.
  - Complete serious incident notification if criteria met. Read more here.
- **Cyberbullying**
  - Recognise the patterns of repeated, targeted harm.
  - Address both the harm and the wider context (e.g. school, peer relationships, family).
  - Ensure the impact on the child's mental health and self-esteem is explored.
  - Document evidence systematically.
  - Link to anti-bullying policies and procedures.
- **Digital Neglect**
  - Recognise as a form of neglect requiring intervention.
  - Use the LSCP Neglect Toolkit to assess severity.
  - Consider impact on child's development and wellbeing.
  - Develop appropriate support plan with family.
- **Online Grooming or Exploitation**
  - Treat as a serious safeguarding issue.
  - Follow your organisation's referral procedures (via DSL in education settings and via discussion with safeguarding professionals in health settings) and determine if police involvement is required.
  - Consider digital safety planning and psychological support for the child.
  - Gather and preserve any contextual information but do NOT attempt to access messages or files.
  - Be aware of potential cross-border issues, including jurisdictional challenges where perpetrators operate from outside UK jurisdiction, the need for coordination with CEOP Command and international law enforcement, and ensuring victim support remains the priority regardless of perpetrator location.
  - Complete serious incident notification if criteria met. Read more here.
  - Consider links to Child Sexual Exploitation procedures.
- **Online Radicalisation or Extremist Influence**
  - Follow the Prevent duty referral process within your organisation.
  - Discuss concerns with local Prevent Team.
  - Make a referral to Prevent using the National Referral Form.

  - Recognise that radicalisation is a form of coercive control, and support must be non-punitive and child-centred.
  - Consider the role of family and peer influences.
- **AI-Generated or Deepfake Abuse**
  - Respond as you would to image-based abuse.
  - Escalate in line with your organisation's safeguarding procedures and consider a police referral.
  - Provide reassurance and specialist support to affected children.
  - Recognise the unique trauma that digital replication may cause.
  - Consider need for specialist therapeutic support.
- **Cross-Border Online Harm**
  - Recognise jurisdictional challenges.
  - Liaise with the National Crime Agency where appropriate.
  - Ensure victim support regardless of perpetrator location.
  - Consider international cooperation through appropriate channels (NCA should advise).
  - Coordinate with police and children's services in other UK areas where the child has connections.
  - Share intelligence about online networks operating across local authority boundaries.
  - Consider whether online exploitation is part of organised criminality.
- **Disruption of Online Perpetrators**
  - Consider full range of civil orders and disruption tools available.
  - Ensure Child Abduction Warning Notices (CAWNs) are monitored for effectiveness.
  - Pursue victimless prosecutions where possible and appropriate.
  - Consider National Referral Mechanism (NRM) referrals for online exploitation.
  - Coordinate disruption activities with relevant agencies across jurisdictions.

Where there is harmful content of a child online, practitioners should endeavour to remove this content by:

- Working with platforms and relevant agencies to remove harmful content, particularly self-harm or exploitation imagery.
- Support the child to access Report Remove.
- Document all attempts at content removal and outcomes.
- Recognise the challenges in removing content but pursue all available avenues.
- Consider multi-agency approaches involving police and platform providers.
- In the case of material promoting terrorism or extremism, make a report to the Counter Terrorism Internet Referral Unit.

Appendix C provides a range of direct work and safety planning support tools to help respond to online risk.

The remainder of this section explores vulnerability-informed approaches to online risk. It includes:

- Understanding of specific vulnerabilities
- Recognition and assessment of online risk
- Adaptive interventions
- Professional practice considerations

These factors should be considered when completing the Online Safety Risk Assessment Template with reference to Appendix A which provides comprehensive trait manifestation tables and detailed vulnerability analysis.

7.1 Responding to neurodivergent children

(A) Understanding specific vulnerabilities

ADHD - Research shows that children with ADHD are 2x more likely to experience online victimisation, with dopamine seeking driving platform engagement and executive function challenges affecting safety decisions. ADHD traits which can increase online risk include impulsivity, hyperactivity, inattention, emotional dysregulation, hyperfocus, time blindness, and rejection sensitivity all create specific online vulnerabilities.

Autism - Research show that autistic children are 2-3x more likely to experience online sexual victimisation, with literal interpretation of communication and difficulty detecting deception creating vulnerability. Autistic traits which can increase online risk include literal thinking, social naivety, intense interests, need for routine, sensory differences, and honesty all create specific online vulnerabilities.

Multiple neurodivergent traits - Many children present with combinations of neurodivergent traits – whether through formal dual diagnosis, traits of one condition alongside a diagnosis of another, or multiple traits that don't meet specific diagnostic thresholds. These children may be particularly vulnerable as they experience compounding effects, such as impulsivity + literal thinking = immediate trust of strangers

(B) Recognition and assessment of risk

Neurodivergent children's online activity may present differently from traditional online risk indicators. For example:

- *Hyperfocus* rather than secretive device use;
- *Emotional dysregulation from overstimulation* rather than concerning content;
- *Special interest communities* feeling like "real friends";
- *Communication differences* rather than defensive behaviour.

Assessment should prioritise the following questions:

- How do their specific traits manifest online?
- Are their traits being exploited by platforms or individuals?

- What needs are they meeting online?
- How do they process online information differently?

(C) Adapting interventions

The core principles of assessment are:
1. **Collaborative** – Work WITH their traits, not against them
2. **Realistic** – They WILL go online, so plan for this reality
3. **Strengths-based** – Use their abilities and interests
4. **Sustainable** – They must be able to maintain any plan you use

Key intervention approaches:
- *For ADHD*: "Quick Check" system with visual reminders and physical prompts before posting/sharing
- *For Autism*: Clear, specific rules integrated into routines (e.g., "Only accept friend requests from people you've met offline")
- *The Balance Sheet Approach*: Help children understand what online spaces give them and how safety measures can preserve beneficial connections

(D) Professional Practice

Use language that supports:
- "connection-seeking" rather than "attention-seeking",
- "struggling to stay safe" rather than "placing himself/herself/themself at risk",
- "needs adapted approach" rather than "won't follow rules".

Ask these reflective questions:
- What need is the online behaviour meeting?
- How do their neurodivergent traits influence their online choices?
- Have we adapted our approach for their neurodiversity?
- Would our plan work for a neurodivergent child?

7.2 Responding to children who are looked after

(A) Understanding specific vulnerabilities

Children who are looked after face specific online vulnerabilities due to their care experience, including connection-seeking behaviour, reduced family protection, and the impact of historical trauma on their ability to recognise unsafe relationships.

Key risk factors include placement disruption, limited family support, identity uncertainty, historical trauma, transition anxiety, and need for control all create specific online vulnerabilities.

Specific online risks include:

- Targeted exploitation by adults who specifically seek vulnerable children needing belong and stability.
- Unsafe family contact arrangements through digital platforms that may lack proper safeguards.
- Inappropriate sharing of placement information, locations or care arrangements.
- Risky peer networks with other children in care may normalise unsafe behaviours.

(B) Recognition and assessment of risk

The online activity of children who are looked after may present differently from traditional online risk indicators. For example:

- *Privacy-seeking* after loss of autonomy rather than secretive device use
- *Legitimate support networks* rather than concerning "new online friends"
- *Placement-related emotions* rather than concerning online content reactions
- *Response to monitoring* rather than defensive behaviour about online activity.

Assessment should prioritise the following questions:

- How does their care experience influence their online choices?
- What connection or belonging needs are being met online?
- How does placement stability affect their online behaviour?
- Are they seeking family relationships or substitute connections?

(C) Adapting interventions

The core principles of assessment are:

1. **Relationship-Focused** – Build trust before imposing restrictions
2. **Trauma-Informed** – Understand behaviour in context of care experience
3. **Autonomy-Respectful** – Balance safety with age-appropriate independence
4. **Stability-Promoting** – Use online safety as tool for building security

Key intervention approaches:

- Safe Connections Approach: Approved contact lists with family, friends, and other children in care (with safeguards), plus connection safety rules about sharing placement details.
- Digital Stability Framework: Consistent safety rules across placements, portable safety plans, and maintained beneficial relationships during transitions.
- Carer Support: Training on CLA-specific vulnerabilities, balancing safety with relationship-building, and gradual increase in online independence.

(D) Professional Practice

Use language that supports:

- "connection-seeking" rather than "attention-seeking online,"
- "struggling with digital boundaries" rather than "won't follow our rules,"
- "needs support to stay safe" rather than "puts himself/herself/themself at risk."

Ask these reflective questions:
1. How does their care experience influence their online choices?
2. What attachment or belonging needs are being met online?
3. Are we balancing safety with their need for connection?
4. How does online safety integrate with their overall care plan?

Practitioners should also ensure online safety integrates with care planning, all professionals understand CLA-specific risks, and there's consistency across placements with appropriate specialist support.

7.3 Responding to children affected by domestic abuse

(A) Understanding specific vulnerabilities

Children affected by domestic abuse face specific online vulnerabilities due to exposure to technology-facilitated abuse, normalised controlling behaviours, and the dual nature of online spaces as both escape and additional risk.

Key risk factors include technology monitoring by perpetrators, normalised control patterns, isolation from support networks, trauma responses affecting risk recognition, seeking escape online, and exposure to abusive relationship models all create specific online vulnerabilities.

Specific online risks include:
- Technology-facilitated abuse including monitoring, location tracking, and digital coercive control
- Normalised controlling behaviours making online control seem acceptable or normal
- Isolation tactics preventing access to online support to help-seeking
- Pattern replication where children may accept similar controlling behaviours from online contacts

(B) Recognition and assessment of risk

Children affected by domestic abuse may present differently from traditional online risk indicators:
- *Excessive privacy concerns* due to fear of monitoring rather than secretive behaviour
- *Reluctance to seek help online* due to fear of discovery rather than lack of awareness of help available
- *Normalised controlling behaviour* in online relationships rather than recognising red flags
- *Fear-based responses* to safety planning rather than resistance to advice.

Assessment should prioritise the following questions:
- How does the domestic abuse situation affect their online behaviour?
- Are they being monitored or controlled through technology?

- What online spaces provide escape or support?
- How does exposure to abuse affect their recognition of online risks?

(C) Adapting interventions

The core principles of assessment are:
1. **Safety-First** – Recognise that a perpetrator may monitor online activity
2. **Trauma-Informed** – Understand behaviour in context of abuse exposure
3. **Empowerment-Focused** – Build autonomy while maintaining safety
4. **Coordinated** – Integrate with domestic abuse support services

Key intervention approaches:
- Covert Safety Planning: Discrete safety measures that don't alert perpetrators, including private browsing techniques and safe communication methods.
- Digital Independence Building: Gradual development of safe online autonomy, separate accounts unknown to perpetrators, and secure communication with support services.
- Support Network Development: Connection with domestic abuse services, online peer support groups (safely facilitated), and maintaining beneficial relationships while ensuring safety.

(D) Professional Practice

Use language that supports:
- "struggling to stay safe online" rather than "putting himself/herself/themself at risk",
- "learned responses to control" rather than "attention-seeking behaviour",
- "safety planning" rather than "restriction of access."

Ask these reflective questions:
1. How does the domestic abuse situation affect their online choices?
2. Are there signs of technology facilitated abuse or control?
3. Are we coordinating with domestic abuse services?
4. How can we support online safety without increasing risk?

Practitioners should ensure coordination with domestic abuse services, police domestic abuse teams, MARAC processes where appropriate, and specialised support services while maintaining information sharing protocols that protect safety

7.4 Responding to children with mental health needs

(A) Understanding specific vulnerabilities

Children with mental health needs face specific online vulnerabilities due to seeking validation and support online, attraction to harmful content during distress, and the dual nature of online spaces as both therapeutic community and risk amplifier.

Key risk factors include crisis-driven online behaviour, vulnerability to harmful content algorithms, seeking validation from strangers, digital self-harm behaviours, isolation driving online connection-seeking, and medication/treatment affecting judgment all create specific online vulnerabilities.

Specific online risks include:

- Harmful content algorithms that amplify depression, anxiety, self-harm, or eating disorder content
- Crisis-driven decision making leading to risky online behaviours during mental health episodes
- Predatory targeting by adults who exploit emotional vulnerability and distress
- Digital self-harm including anonymous negative posting or deliberately seeking distressing content

(B) Recognition and assessment of risk

The online activity of children with mental health needs may present differently from traditional online risk indicators. For example:

- *Increased online activity during distress* rather than withdrawal from devices
- *Seeking harmful content* as form of self-harm rather than accidental exposure
- *Emotional dependency on online validation* rather than healthy social media use
- *Crisis-driven posting* rather than typical risky sharing behaviour

Assessment should prioritise the following questions:

- How does their mental health state affect their online behaviour?
- Are they seeking harmful content or communities during distress?
- What online support is beneficial vs. concerning?
- How do mental health crises correlate with online risk-taking?

(C) Adapting interventions

The core principles of assessment are:

1. **Therapeutic** - Balance safety with mental health support needs
2. **Crisis-Responsive** - Adapt safety planning for mental health episodes
3. **Dual-Aware** - Recognise online spaces as both help and harm
4. **Coordinated** - Integrate with mental health treatment services

Key intervention approaches:

- Crisis Safety Planning: Alternative coping strategies for distressing moments, safe online support contacts for crisis periods, and harmful content blocking during vulnerable times.
- Beneficial Community Connection: Facilitated access to positive peer support groups, moderated mental health communities, and therapeutic online resources while maintaining safety.

- Algorithm Awareness: Understanding how platforms amplify certain content, techniques for resetting feeds toward positive content, and recognition of when algorithms become harmful

(D) Professional Practice
Use language that supports:
- "seeking connection during distress" rather than "attention-seeking online",
- "struggling with digital coping" rather than "addicted to social media",
- "needs support for online safety" rather than "makes poor online choices."

Ask these reflective questions:
1. How do mental health episodes affect their online behaviour?
2. Are they accessing harmful or helpful online content/communities?
3. How are we coordinating online safety with mental health treatment?
4. What online coping strategies are beneficial vs. concerning?

Practitioners should ensure coordination with CAMHS, mental health services, school counsellors, and therapeutic providers while maintaining crisis response protocols and shared safety planning across services.

7.5 Responding to children experiencing poverty and digital exclusion

(A) Understanding specific vulnerabilities

Children experiencing poverty and digital exclusion face specific online vulnerabilities due to unsafe access methods, limited safety resources, and digital exclusion creating both barriers to online safety information and increased exposure to risks.

Key risk factors include unsafe public Wi-Fi usage, shared device privacy concerns, outdated security software, inability to afford premium safety features, unsupervised public access, and limited data affecting safety feature usage all create specific online vulnerabilities.

Specific online risks include:
- Unsafe access methods including unfiltered public Wi-Fi and unsecured networks in public spaces
- Privacy compromise through shared family devices with family members or in public settings
- Limited safety resources including inability to afford premium accounts with better safety features
- Increased exposure time in unsupervised public spaces with internet access

(B) Recognition and assessment of risk

The online activity of children experiencing poverty and digital exclusion may present differently from traditional online risk indicators. For example:

- *Public space usage* rather than home-based online activity
- *Shared device concerns* rather than personal device secrecy
- *Time-limited access* creating rushed online decisions
- *Basic platform usage* due to inability to access premium safety features

Assessment should prioritise the following questions:
- How do financial constraints affect their online safety options?
- Are they using potentially unsafe access methods?
- What digital inclusion support is needed alongside safety planning?
- How does limited access time affect their online decision-making?

(C) Adapting interventions

The core principles of assessment are:
1. **Inclusive** – Address barriers to accessing safety resources
2. **Practical** – Focus on free and accessible safety solutions
3. **Realistic** – Work within financial and access constraints
4. **Empowering** – Build skills that don't require expensive resources

Key intervention approaches:
- Free Safety Resource Optimisation: Maximising use of free privacy settings, identifying safe public Wi-Fi options, and utilising free safety apps and parental controls.
- Digital Inclusion Support: Connection with device lending schemes, affordable connectivity programmes, and community resources providing safe internet access.
- Time-Efficient Safety Planning: Quick safety checks for limited access time, priority safety actions when time is constrained, and portable safety knowledge that works across different access points.

(D) Professional Practice

Use language that supports:
- "working within access constraints" rather than "poor online choices",
- "limited resources" rather than "can't afford safety",
- "needs digital inclusion support" rather than "digitally excluded."

Ask these reflective questions:
1. How financial constraints affect their online safety options?
2. What barriers exist to accessing safety resources?
3. Are we coordinating with digital inclusion services?
4. How can we maximise free safety resources available?

Practitioners should ensure coordination with family support services, digital inclusion programmes, library services, and community organisations while identifying funding streams for digital safety resources and equipment.

7.6 Responding to children with communication needs and language barriers

(A) Understanding specific vulnerabilities

Children with communication needs face specific online vulnerabilities due to barriers in understanding safety information, difficulty reporting concerns, and challenges in recognising manipulation when communication styles differ from typical online safety assumptions.

Key risk factors include inability to understand safety warnings, difficulty expressing concerns about online experiences, cultural differences in communication norms, language barriers preventing help-seeking, limited access to accessible safety information, and communication disabilities affecting risk recognition all create specific online vulnerabilities.

Specific online risks:

- Safety information barriers including inability to access or understand standard online safety guidance
- Reporting difficulties when children cannot effectively communicate concerns about online experiences
- Cultural vulnerability where different communication norms may be exploited by perpetrators
- Support access barriers preventing effective help-seeking when problems arise

(B) Recognition and assessment of risk

The online activity of children with communication needs and language barriers may present differently from traditional online risk indicators. For example:

- *Frustration with safety discussions* due to communication barriers rather than resistance
- *Continued risky behaviour* after safety education due to comprehension rather than defiance
- *Reluctance to report problems* due to communication difficulties rather than secrecy
- *Family involvement in all online activity* due to communication support needs rather than control

Assessment should prioritise the following questions:

- Do they understand online safety information in formats they can access?
- Are cultural or language barriers preventing them from seeking help?
- What interpretation or accessible communication support is needed?
- How do their communication needs affect their ability to recognise online risks?

(C) Adapting interventions

The core principles of assessment are:

1. **Accessible** – Ensure all safety information is available in appropriate formats
2. **Culturally-Responsive** – Respect diverse communication styles and norms
3. **Supported** – Provide interpretation and communication assistance
4. **Visual** – Use non-verbal communication methods where appropriate

Key intervention approaches:

- Visual Safety Planning: Picture-based safety plans with photos of safe adults, visual examples of safe/unsafe messages, and step-by-step visual guides for blocking and reporting.
- Accessible Communication: Safety information in multiple languages, easy-read formats, BSL interpretation, and cultural mediators for family discussions about online safety.
- Supported Reporting: Clear and accessible reporting mechanisms, trusted adult identification with communication support, and alternative reporting methods (visual, supported, translated).

(D) Professional Practice

Use language that supports:

- "needs communication support" rather than "doesn't understand safety",
- "requires accessible information" rather than "won't follow advice"
- "communication barriers" rather than "language problems."

Ask these reflective questions:

1. Do they have access to online safety information in accessible formats?
2. What communication support is needed for safety planning?
3. Are we working with interpretation services and cultural mediators?
4. How can we adapt our communication to match their needs?

Practitioners should ensure coordination with interpretation services, cultural community organisations, SEND services, and speech and language therapy while maintaining accessible communication throughout all professional interactions

8. Supervision & Reflection

Reflective questions inform good quality assessments and reviews. Practitioners can consider these questions as a self-reflective exercise and in supervision spaces.

Universal Questions:

- How does this child use online spaces for emotional regulation?
- What would be lost if online access was restricted?
- How can we reduce risk while maintaining beneficial connections?
- What offline needs are being met online?
- Have we considered that social media might be their main coping strategy?

Understanding the Behaviour:

- What need is the online behaviour meeting?
- How do their specific vulnerabilities influence their online choices?
- What offline factors push them online?
- Have we assessed capacity to understand risk?
- Are there signs of digital neglect that need addressing?

Checking Our Response:

- Are we balancing safety with wellbeing?
- Have we adapted our approach for their specific vulnerabilities?
- Are we seeing behaviour through a trauma lens?
- Is our plan realistic for their cognitive/executive function?

Multi-Agency Effectiveness:

- Does everyone understand the vulnerability impact?
- Are we duplicating or missing anything?
- Who's leading on disruption?
- When did we last review what's working?

When Cases Feel Overwhelming:

- Name the dual challenge (online risk + neurodiversity)
- Share responsibilities across team
- Focus on small, achievable changes
- Celebrate incremental progress
- Access specialist consultation

Self-Care for Complex Cases:

- Regular supervision is essential
- Share exposure to harmful content and seek support where needed
- Debrief after difficult disclosures
- Access counselling/support as needed
- Create protected time for reflection

8.1 Vulnerability-Specific Questions

The following questions should also be asked dependent on the vulnerability of the child.

***For Neurodivergent Children*:**

- How do their specific neurodivergent traits (for example, but not restricted to, ADHD impulsivity, autistic literal thinking, sensory needs) affect their online choices and vulnerability?
- Are their special interests, need for routine, or online emotional regulation being exploited or creating risk?
- What adaptations are needed to make safety planning and advice work for their specific processing style and presentation?

For Looked-After Children:

- How does their care experience effect their online connection-seeking?
- Are they using online spaces to maintain relationships disrupted by placement moves?
- How can we support safe online relationships while in care?

For Children Affected by Domestic Abuse:

- Are there signs of technology-facilitated abuse or control?
- How does the perpetrator's digital behaviour affect this child?
- What online safety needs does the non-abusive parent have?

For Children with Mental Health Needs:

- How does this child's mental health affect their online choices?
- Are they being drawn to harmful content during times of distress?
- What online support networks are beneficial vs. concerning?

For Children Experiencing Poverty:

- How do financial constraints affect this child's online safety options?
- Are they using potentially access methods due to cost barriers?
- What digital inclusion support is needed alongside safety planning?

For Children with Communication Needs:

- Do they understand online safety information in formats they can access?
- Are cultural or language barriers preventing them from seeking help?
- What interpretation or accessible communication support is needed?

9. Multiagency response and coordination

Where assessment has identified a child is at risk of, or is experiencing, online harm there is a need for effective multi-agency responses.

All multi-agency working must follow the requirements outlined in the London Safeguarding Children Procedures and Working Together to Safeguard Children.

To address online risk, multiagency working should include a vulnerability-informed agenda, by seeking to establish:

1. What vulnerabilities does this child have and how do they affect online behaviour?
2. What platforms/patterns have been identified?
3. What's working/not working in current approach?
4. How do we adapt standard safety advice for their specific needs?
5. Who leads on new action?
6. When do we review?

Any actions identified need to be SMART (Specific, Measurable, Achievable, Relevant, Time-bound). For example:

☒ *Standard Action:*
"Educate the child about online safety

☑ *Vulnerability-Adapted SMART Action:*
"SENCO (or equivalent educational professional) and Social Worker will create visual online safety rules specific to Instagram, using child's special interest (anime) as examples, by [date]. Parents will reinforce using the agreed reward system."

10. Intervention and support: learning from practice

Disclaimer: These are composite case examples based on research and practice themes. Names and identifying details have been changed.

Case Study 1: Jamie (ADHD + Care Experience)

Background:
Jamie, 14, diagnosed with ADHD, had been in foster care for 8 months following family breakdown. Known for emotional dysregulation during transitions and placement moves.

Incident:
During a particularly difficult weekend when placement was under review, Jamie impulsively started livestreaming on TikTok, announcing they were "running away for good" and showing recognisable local landmarks. The stream ran for over 3 hours with location services enabled. Multiple unknown adults in the chat offered "help," suggesting meeting places and offering accommodation. Foster carer discovered the stream when Jamie didn't come down for dinner.

How ADHD and Care Experience Increased Risks:
ADHD Factors:

- Impulsive decision making when emotionally dysregulated - no pause to consider consequences
- Hyperfocus on viewer comments provided dopamine hit during distress
- Time meant Jamie lost track of how long they'd been streaming
- Rejection sensitivity drove them to overshare personal details to maintain viewer engagement
- Executive function challenges meant they couldn't plan how to stay safe while streaming

Care Experience Factors:

- Placement uncertainty created heightened emotional distress and need for external validation
- Limited consistent support network meant fewer trusted adults to turn to during crisis
- Previous placement disruptions had normalised uncertainty, making online "offers of help" seem appealing
- Seeking belonging and stability made Jamie vulnerable to adults offering permanent relationships
- Reduced family protection meant less immediate supervision during the crisis period

Combined Impact:

- ADHD impulsivity + placement anxiety = immediate broadcasting of distress without safety considerations
- Need for validation + care experience of instability = accepting attention from strangers offering "help"
- Executive function difficulties + limited support network = inability to access safer coping strategies
- Emotional dysregulation + placement review stress = crisis livestreaming as only available outlet

What Worked:

Immediate Response:

- Foster carer had established "code word" system - used this in chat comments to identify themselves safely
- Police were able to trace Jamie's location via the platform while foster carer kept them engaged online

ADHD-Informed Interventions:

- Created specific "impulse interruption" plan with visual prompts on Jamie's devices
- Alternative: Introduced a private voice recording app where Jamie could vent emotions without broadcasting
- Developed a reward system for Jamie checking in during emotional moments

LAC-Informed Interventions:

- Worked with Jamie to identify triggers related to placement uncertainty
- Established consistent check-in routine with trusted adults during stressful periods
- Connected Jamie with other care-experienced children who had developed healthy coping strategies
- Integrated online safety planning into overall care planning and placement stability work
- Ensured all placement moves included transfer of safety planning and trusted adult relationships

Key Learning:

Jamie needed both ADHD-specific strategies for impulsive moments AND CLA-specific support for placement-related distress. Standard “don’t livestream” advice was completely inadequate for a child experiencing both neurodivergent traits and care-related trauma. Success came from addressing both vulnerability types simultaneously - providing immediate emotional regulation tools for ADHD while building placement stability and trusted relationships for care experience needs.

Case Study 2: Alex (Autism + Communication Needs)

Background:
Alex, 13, was autistic with intense special interest in anime, particularly rare manga collections. Socially isolated at school, Alex found most meaningful connections in online anime communities. Alex's family had recently moved to the UK, with parents having limited English and limited understanding of online risks or UK safeguarding systems.

Incident:
Adult "mentor" in specialist anime forum built a relationship with Alex over 6 months through detailed discussions about rare manga. Gradually introduced "fair trade" concept – offering rare digital manga in exchange for increasingly inappropriate photos of Alex. Alex saw this as logical exchange between collectors and trusted the adult's expertise about anime values. However, as the requests became more inappropriate and the adult became more insistent and demanding, Alex began to feel uncomfortable but struggled to understand why something that had seemed like a fair trade now felt wrong. When Alex tried to discuss concerns with parents, their unfamiliarity with online risks and UK safeguarding systems, combined with cultural differences about discussing personal matters, meant the situation continued unaddressed.

How Autism and Communication Needs Increased Risk:
Autism Factors:

- Literal thinking meant Alex interpreted "fair trade" concept literally
- Social naivety prevented recognition that the adult had ulterior motives
- Strong rule-following trait meant believed that "They helped me first, so I should help them"
- Special interest created deep trust in anyone with anime knowledge
- Difficulty detecting deception in text-based communications
- Black-and-white thinking about loyalty and reciprocity made it difficult for Alex to step away from unreasonable and abusive requests

Communication Needs Factors:

- Parents' limited English meant they couldn't access UK online safety information or understand platform risks
- Family unfamiliarity with UK safeguarding systems meant they didn't know how to seek help when Alex raised concerns
- Cultural differences about discussing personal/physical matters made it difficult for Alex to fully explain what was happening
- No access to safety information in family's first language meant parents couldn't educate themselves about online risks
- Parents' unfamiliarity with social media and online platforms meant they couldn't assess the situation Alex described
- Language barriers prevented parents from communicating effectively with UK professionals when help was eventually sought

Combined Impact:

- Autism literal thinking + cultural unfamiliarity = accepting "trading" as normal business practice
- Special interest trust + parents' unfamiliarity with online platforms = concerns dismissed or misunderstood when discussed
- Social naivety + cultural isolation = no alternative perspectives to challenge the relationship
- Communication difficulties + family unfamiliarity with UK systems = delayed help-seeking when concerns arose

What Worked:

Immediate Response:

- Used a visual flowchart to explain exploitation (not abstract concepts about manipulation)
- Provided materials in family's first language to help parents understand what had occurred

Autism-Informed Interventions:

- Created concrete, specific rules, e.g.: “Never send phots of yourself – real collectors charge money for what they are selling”
- Arranged supervised participation in verified anime groups with clear moderation in place
- Connected Alex with an older, trusted autistic anime fan as a peer mentor who understood both autism and the anime culture
- Developed a “red flag” visual guide specific to trading scenarios

Communication Needs-Informed Interventions:

- Worked with cultural mediator to help family understand online risks within their cultural context
- Provided online safety information in family's first language and easy-read formats for Alex
- Connected family with community organizations that could provide ongoing support in their language
- Established clear communication methods for Alex to report concerns using visual aids and simple language
- Developed safety planning that respected cultural values while maintaining protection

Key Learning:

Alex needed both autism-specific understanding of literal thinking and trust patterns AND culturally-responsive communication support for the whole family. Standard online safety education failed because it didn't account for either autism processing differences or the family's language and cultural needs. Success required addressing both the individual's neurodivergent presentation and the family's communication barriers simultaneously.

Case Study 3: Maya (Mental Health Needs + Domestic Abuse)

Background:
Maya, 15, had been receiving CAMHS support for depression and anxiety for the past year. She lived with her mother and stepfather, with social services previously involved due to domestic abuse incidents. Maya used social media extensively for emotional regulation and found online communities where she felt understood and validated during difficult periods.

Incident:
During a particularly challenging period when domestic abuse incidents at home had escalated, Maya began posting increasingly personal content about her emotional state on various platforms. An adult began commenting supportively on her posts, gradually moving conversations to private messaging. Over several weeks, this adult gained Maya's trust by offering emotional support and understanding about her mental health struggles. The adult then began requesting personal information and photos, framing these requests as "helping her feel better about herself" and "showing she was special." Maya, desperate for validation during a mental health crisis and isolated due to the domestic abuse situation, complied with increasingly inappropriate requests.

How Mental Health Needs and Domestic Abuse Increased Risk:
Mental Health Factors:

- Depression and anxiety made Maya particularly vulnerable to seeking validation from any source offering support
- Crisis periods led to impulsive posting and sharing without considering safety implications
- Low self-esteem made compliments and attention from the adult particularly powerful
- Difficulty with emotional regulation meant Maya couldn't assess the appropriateness of requests objectively
- Mental health episodes created desperate need for external validation and support
- Online spaces had become primary coping mechanism for managing difficult emotions

Domestic Abuse Factors:

- Chaotic home environment meant less consistent supervision of online activity
- Maya couldn't discuss concerns about online contact due to fear of perpetrator monitoring devices
- Isolation from support networks due to domestic abuse made online validation more significant
- Trauma responses meant Maya normalised inappropriate attention and boundary violations
- Experience of coercive control at home made similar patterns online seem familiar rather than alarming
- Fear of disclosing to authorities due to potential consequences for family situation

Combined Impact:

- Mental health crisis + domestic abuse isolation = accepting any positive attention regardless of source
- Emotional vulnerability + learned patterns of coercion = unable to recognise grooming techniques
- Need for validation + fear of monitoring = continuing unsafe online relationships in secret
- Depression symptoms + chaotic home environment = impulsive online behaviour without safety considerations

What Worked:

Immediate Response:

- CAMHS worker recognised changes in Maya's presentation and directly asked about online experiences
- Safety planning included digital safety considerations alongside mental health support

Mental Health-Informed Interventions:

- Developed alternative sources of validation and support through peer groups and therapeutic relationships
- Created safety planning specifically for mental health crisis periods, including online behaviour guidelines
- Worked on emotional regulation techniques that didn't rely solely on external online validation
- Connected Maya with moderated online mental health support groups with appropriate safeguards

Domestic Abuse-Informed Interventions:

- Coordinated with domestic abuse services to address the underlying trauma and safety concerns
- Developed discrete safety planning that wouldn't alert perpetrator to intervention
- Provided safe communication methods for Maya to report online concerns without risk of monitoring
- Addressed trauma responses that made boundary violations seem normal or acceptable
- Worked with mother separately to address domestic abuse situation and improve home safety

Key Learning:

Maya needed both mental health crisis support that addressed her need for validation AND domestic abuse-informed intervention that understood how trauma affected her online vulnerability. Standard online safety advice failed because it didn't account for either her emotional desperation during mental health episodes or her learned responses to coercive control. Success required coordinating mental health treatment with domestic abuse support while developing alternative coping strategies that met her emotional needs safely.

11. Resources and Tools

Please see Appendix C for a list of direct work tools which can be used with children.

11.1 Safer Schools App

Lambeth Schools can access the Safer Schools App for free. This includes up to date information, alerts and prompts, CPD online safeguarding courses and teaching resources.

11.2 National Resources

For practitioners:

- CEOP Education: age-appropriate safety resources
- UK Safer Internet Centre: professional guidance and training
- NSPCC Online Safety Hub: information and resources to help talk to children about online safety
- SWGfL: educational safeguarding resources
- SWGfL Professionals Online Safety Helpline: 0344 381 4772
- Internet Watch Foundation: reporting harmful content

For Families:

- Internet Matters: platform-specific guidance and parental controls
- Parent Zone: family online safety advice
- Childnet: educational resources for families
- NSPCC Online Safety Hub: information and resources to help talk to children about online safety
- Common Sense Media: age ratings and reviews

For Children:

- Childline: 0800 1111 - Confidential support
- Report Remove: help removing self-generated images
- CEOP Report: report concerning online contact
- Young Minds: mental health support including online wellbeing

11.3 Vulnerability-Specific Resources

Neurodivergent Children:

- ADHD Foundation**:** ADHD-specific online safety information
- The National Autistic Society: Autism-specific online guidance

Children Affected by Domestic Abuse:

- Women's Aid: Technology safety resources
- Refuge Tech Safety**:** Digital safety planning resources

Children with Communication Needs:

- Mencap: Easy-read online safety resources

Children with Mental Health Needs:

- Young Minds Crisis Messenger**:** Text YM to 85258
- Kooth: App to support children with mental health needs
- Samaritans**:** 116 123

All Vulnerabilities:

- Act Early: Safeguarding guidance including online safety

11.4 Professional Development

Training Resources:

- LSCP Training Programme - Contact for current online safety training courses
- UKCIS (UK Council for Internet Safety)
- Project Evolve**:** Progressive online safety education framework
- SWGfL 360 Safe: Organisational online safety assessment

11.5 Key Contacts

- Immediate Risk**:** 999
- CEOP
- Lambeth Children's Social Care:
    - 0207 925 3100 (office hours)
    - 0207 926 555 (out of hours)
    - helpandprotection@lambeth.gov.uk
    - Referral form

11.6 Reporting Harmful Content

- Report Remove (for self-generated images)**:**
- Individual platform reporting: Check platform safety centres
- Counter Terrorism Internet Referral Unit**:** For material promoting terrorism or extremism

11.7 Further reading and guidance

- LSCP Online Safety Policy
- Child sexual abuse material generated by artificial intelligence - an essential guide for professionals who work with children
- Sharing nudes and semi-nudes guidance

Remember: These resources support vulnerability-informed practice. Always consider the child's specific vulnerabilities when selecting appropriate resources and adapt guidance to match their needs and capabilities.

12. Conclusion: Changing the Paradigm

This guidance represents a paradigm shift in how we approach online safety for vulnerable children, moving beyond generic approaches to recognise digital harm and digital neglect as serious safeguarding concerns requiring specialist responses.

We must move from: "*Child with vulnerabilities who happens to be at risk online*"

To: "*Child whose specific vulnerabilities directly shapes their online experience and require specifically adapted safety approaches, with digital neglect recognised as a form of neglect requiring intervention*"

Your Challenge

Starting tomorrow, how will you differently approach online safety for vulnerable children?

- For the neurodivergent child: Will you consider how their traits specifically manifest online?
- For the child who is looked after: Will you understand their connection-seeking as a legitimate need?
- For the child affected by domestic abuse: Will you recognise technology-facilitated control?
- For the child with mental health needs: Will you see online spaces as both risk and lifeline?
- For the child experiencing poverty: Will you address digital exclusion alongside safety?
- For the child with communication needs: Will you ensure your safety guidance is accessible?
- For any child with multiple vulnerabilities: Will you coordinate responses that address their whole experience?

Appendix A: Trait Manifestation Tables and Vulnerability Analysis

A.1: Neurodivergent Children

ADHD Traits Manifestation Table:

ADHD Trait	Online Manifestation	Increased Risk
Impulsivity	Quick decisions about sharing/meeting	Personal data exposed, unsafe meetings
Hyperactivity	Excessive posting, multiple platforms	Larger digital footprint, more exposure
Inattention	Missing warning signs, forgetting privacy	Grooming, unnoticed, accounts compromised
Emotional dysregulation	Posting when upset, seeking validation	Vulnerability when distressed, oversharing
Time blindness	Lost in scrolling, marathon sessions	Extended exposure to risks
Rejection sensitivity	Desperate for likes/followers	Accepting unsafe connections
Executive dysfunction	Difficulty planning safe online behaviour, struggling with consequences	Poor safety decision-making, inability to learn from mistakes
Hyperfocus	Becoming completely absorbed in online activities or relationships	Missing danger signs, ignoring safety advice

Autistic Traits Manifestation Table:

Autistic Trait	**Online Manifestation**	**Increased Risk**
Literal thinking	Taking statements at face value, missing sarcasm or deception	Vulnerable to manipulation and grooming
Social naivety	Not recognising ulterior motives, trusting online contacts easily	Exploitation by predators
Intense interests	Deep engagement in specific online communities, sharing detailed knowledge	Being targeted through special interests
Need for routine	Using same platforms at predictable times, following patterns	Stalking, location tracking, behavioural prediction
Sensory differences	Preference for text-based communication over video calls	Missing non-verbal danger cues and social context
Honesty	Oversharing personal information, being truthful about details	Identity theft, targeting, personal safety risks
Rule-following	Believing they must comply with requests from "authority" figures	Exploitation by those claiming expertise or authority
Social communication differences	Difficulty reading online social cues and intentions	Misunderstanding dangerous situations

Multiple Neurodivergent Traits

Trait Combination	Compound Risk	Example Scenario
Impulsivity + Literal thinking	Immediate acceptance of dangerous requests	Quickly agreeing to meet someone who claims to be a "friend"
Special interests + Hyperfocus	Extreme vulnerability in niche communities	Spending hours with online "mentor" in gaming community
Social difficulties + Rejection sensitivity	Accepting any positive attention	Continuing unsafe relationship because it's only source of validation
Executive dysfunction + Need for routine	Inability to change unsafe patterns	Continuing to use compromised platforms or contacts
Sensory preferences + Social naivety	Missing danger signs in preferred communication	Not recognizing grooming in text-only conversations

A.2: Children Looked After

Care Experience Factor Manifestation Table:

Core Experience Factor	Online Manifestation	Increased Risk
Placement disruption	Seeking stable online relationships during placement changes	Vulnerable to grooming offering "permanent" relationships
Limited family support	Accepting positive attention from any online source	Trusting strangers who show consistent interest
Identity uncertainty	Experimenting with different online personas, seeking belonging	Sharing personal information inappropriately
Historical trauma	Normalising inappropriate online behaviour and boundary violations	Not recognising grooming or exploitation patterns
Transition anxiety	Seeking reassurance during placement moves or life changes	Increased vulnerability during stressful periods/placement moves
Need for control	Taking online risks to feel autonomous after institutional control	Rejecting safety advice as "more control"
Attachment difficulties	Forming intense online relationships quickly	Dangerous emotional dependence on online contacts
Care system knowledge	Understanding of "system language" may be exploited	Adults using care system knowledge to build false trust

Placement-Related Vulnerability Patterns:

Placement Type	Specific Online Vulnerabilities	Risk Factors
Foster care	Sharing placement details, seeking birth family online	Location disclosure, unsafe family contact
Residential care	Peer pressure for risky online behaviour, shared device issues	Group risk-taking, privacy compromise
Kinship care	Complex family dynamics affecting online relationships	Conflicted loyalties, family boundary issues
Independent living	Reduced supervision, increased online freedom	Less support during online crises
Placement breakdown	Crisis-driven online behaviour, seeking immediate alternatives	Desperate decision-making, accepting unsafe offers

A.3: Children Affected by Domestic Abuse

Technology-Facilitated Abuse Patterns:

Abuse Tactic	Online Manifestation	Impact on Child
Monitoring	Checking child's devices, tracking online activity	Trusting strangers who show consistent interest
Isolation	Preventing online contact with friends/family	Increased dependency on abuser for social contact
Coercive control	Controlling what platforms child can use	Limited access to support resources
Intimidation	Threatening consequences for online behaviour	Fear-based compliance with restrictions
Financial abuse	Controlling access to internet/devices	Unsafe public access, limited safety resources
Image-based abuse	Sharing or threatening to share intimate images	Shame, compliance through fear
Stalking	Tracking location through devices, monitoring social media	No sense of safe space, even online
Impersonation	Creating fake accounts to monitor or contact child	Confusion about who can be trusted online

Trauma Response Manifestations Online:

Trauma Response	Online Behaviour	Vulnerability Created
Hypervigilance	Constantly checking for threats, monitoring perpetrator online	Exhaustion, missing other risks
Emotional numbing	Reduced emotional response to inappropriate requests	Not recognizing dangerous situations
Dissociation	"Checking out" during online interactions	Poor decision-making during episodes
Learned helplessness	Not reporting online abuse, accepting inappropriate behaviour	Continued victimization
Complex trauma bonding	Seeking relationships that mirror abuse dynamics	Attracted to controlling online relationships
Survival mode thinking	Making decisions based on immediate safety, not long-term consequences	Risky choices for short-term relief

A.4: Children with Mental Health Needs

Mental Health Crisis Manifestations Online:

Health State	Online Behaviour	Increased Risk
Depression episode	Seeking validation, posting negative content about self	Vulnerable to predators exploiting low mood
Anxiety spike	Compulsive checking, seeking reassurance online	Susceptible to manipulation through fear
Manic episode	Impulsive posting, oversharing, risky online behaviour	Poor judgment, dangerous disclosures
Self-harm urges	Seeking self-harm content, joining harmful communities	Escalation of self-destructive behaviour
Suicidal ideation	Researching methods, seeking "support" for harmful plans	Dangerous content exposure, harmful encouragement
Eating disorder behaviours	Engaging with pro-eating disorder content and communities	Reinforcement of harmful behaviours
PTSD triggers	Dissociation during online activity, seeking trauma-related content	Poor decision-making, re-traumatisation
Emotional dysregulation	Extreme mood swings affecting online judgment	Unpredictable risky behaviour

Platform Algorithm Vulnerability Patterns:

Mental Health Need	Algorithm Risk	Harmful Content Amplification
Depression	Negative content reinforcement	Self-harm, suicide content, hopelessness
Anxiety	Fear-based content amplification	Catastrophic thinking, panic triggers
Eating disorders	Body image and diet content	Pro-eating disorder communities, harmful comparison
PTSD	Trauma-related content	Re-traumatisation, trigger exposure
Self-harm	Related content suggestion	Escalation of harmful behaviours
Social anxiety	Avoidance-enabling content	Further isolation, reduced real-world interaction

A.5: Children Experiencing Poverty and Digital Exclusion

Digital Exclusion Impact Analysis:

Poverty Factor	Online Impact	Safety Vulnerability
Limited income	Reliance on free public Wi-Fi	Unfiltered, unsecured internet access
Shared devices	No private internet access	Compromised privacy, inability to seek help safely
Outdated technology	Lack of current security features	Vulnerable to malware, phishing, exploitation
Data limitations	Restricted internet usage time	Rushed online decisions, unable to research safety
No premium accounts	Limited safety features on platforms	Increased exposure to inappropriate content
Unstable housing	Irregular internet access	Seeking access in unsafe locations
Limited digital literacy	Poor understanding of online risks	Higher vulnerability to scams and exploitation
Language barriers	Limited access to safety information	Unable to understand safety guidance or seek help

Access Barrier Manifestations:

Barrier Type	Online Behaviour	Risk Created
Time-limited access	Rushed decision-making online	Poor safety choices due to time pressure
Public space usage	Using devices in libraries, cafes	Lack of privacy, potential monitoring by others
Shared family devices	Unable to maintain private conversations	Inability to report concerns or seek help
Free platform dependency	Using platforms with fewer safety features	Higher exposure to inappropriate content
No parental controls	Unrestricted access due to inability to afford filtering	Age-inappropriate content exposure
Unsafe location access	Using internet in unsupervised public areas	Physical safety risks, predator targeting
Device sharing with strangers	Borrowing devices from others	Compromised accounts, privacy violations

A.6: Children with Communication Needs and Language Barriers

Communication Barrier Analysis:

Communication Need	Online Manifestation	Safety Vulnerability
Limited English proficiency	Difficulty understanding safety warnings and platform rules	Inability to recognize dangerous situations
Visual impairment	Reliance on screen readers, limited access to visual safety cues	Missing visual warning signs
Hearing impairment	Preference for text-based communication	Missing audio warnings or alerts
Learning disabilities	Difficulty processing complex safety information	Vulnerable to exploitation of comprehension difficulties
Speech difficulties	Preference for written over verbal communication	Limited ability to seek help through voice calls
Cognitive disabilities	Challenges understanding abstract concepts like "grooming"	Difficulty recognizing manipulation tactics
Autism communication differences	Literal interpretation of online communication	Vulnerable to sarcasm, implied threats, or manipulation
Cultural communication norms	Different expectations about privacy and disclosure	Misunderstanding what information is safe to share

Cultural Factor Manifestation:

Cultural Factor	Online Behaviour Impact	Vulnerability Created
Different family privacy norms	Varied expectations about what personal/family information can be shared	Potential mismatch between family sharing practices and online safety guidance
Different authority relationships	Varied comfort levels with questioning adult requests online	Reduced comfort with challenging inappropriate requests
Different privacy boundaries	Individual vs. family-centred privacy expectations	Uncertainty about what information is safe to share online
Gender role expectations	Different online behaviour expectations based on gender	Gender-specific targeting and exploitation
Religious considerations	Seeking faith-based content, trusting religious authorities online	Exploitation through religious manipulation
Community language preferences	Primarily engaging with same-language online communities	Limited access to diverse safety perspectives and support
Immigration status concerns	Fear of reporting problems to authorities	Continued victimisation due to fear of legal consequences
Different educational approaches	Varied expectations about questioning adults or authority figures	Reduced comfort with challenging inappropriate requests

A.7: Intersectional Vulnerability Combinations

Common Multi-Vulnerability Patterns

Vulnerability Combination	Compound Risk Pattern	Intervention Priority
CLA + Neurodivergent	Connection-seeking + processing differences	Relationship-building with adapted communication
Mental Health + Domestic Abuse	Crisis vulnerability + learned trauma responses	Crisis safety planning with trauma-informed approach
Poverty + Communication Needs	Limited access + understanding barriers	Digital inclusion with accessible safety information
Neurodivergent + Mental Health	Processing differences + emotional vulnerability	Specialized support with crisis-responsive planning
CLA + Mental Health	Attachment difficulties + emotional distress	Therapeutic relationship-building with stability focus
Domestic Abuse + Communication Needs	Control/monitoring + inability to seek help	Covert safety planning with accessible communication

Appendix B: Online Safety Risk Assessment Template

Guidance notes
This risk assessment tool should be used to identify, evaluate and manage online risks to children's safety and wellbeing. This tool should be used alongside detailed guidance contained in the LSCP Multiagency Practice Guidance: Online Safety which outlines the types of online risks children might be exposed to and the increased risks associated with specific vulnerability factors, such as children who are neurodivergent, looked after, experiencing mental health needs, etc.

Risk Formulation Framework

- Low risk behaviours are generally safe but still require basic guidance and supervision (e.g. watching age appropriate videos and playing games with only pre-approved friends)
- Medium risk behaviours could become harmful without proper boundaries or awareness (e.g. accepting friend requests from strangers or public posting)
- High risk behaviours indicate a significant risk and require immediate attention and safeguarding responses (e.g. engaging in private conversations with unknown adults or sending/receiving inappropriate messages or images)
- Critical risk behaviours are urgent and potentially life-threatening, requiring immediate safeguarding intervention (e.g. arranging to meet someone they meet online or being involved in criminal activity through online platforms).

Use this formula for systemic risk assessment:
Identified Vulnerabilities + Online Behaviours + Environmental Factors = Overall Risk

Example:

- Recent placement move + Seeking online family + Limited carer support = HIGH RISK
- ADHD impulsivity + Late night posting + Lack of supervision = HIGH RISK
- Stable support + Adapted safety plan + Regular monitoring = LOWER RISK

Consider both individual vulnerabilities and how they interact to create compound risks.

Section 1: Assessment Details

Child Details:

Name:	
Date of Birth:	

Assessment Details:

Assessment Date:	

Assessment Author:	
Agency:	

Section 2: Online Activity Overview

2a) Devices used. *Please list all of the devices the child uses to connect online, for example, smartphones, tablets, games consoles, laptops, etc.*

2b) Platform use and digital behaviour summary. *Please provide an overview of how the child behaves the online world for each platform they connect and engage with.*

Platform (e.g. SnapChat, Tiktok, Roblox, etc).	Average daily time spent on platform	Primary Use (i.e. what is the primary reason or purpose for using the platform)	Key Contacts (i.e. who are they talking to?).	Type of risk (content, contact, conduct or commerce)?

2c) Supervision. *Please describe any supervision of the child's online activity including parental controls, any enforced 'offline-time', checking of profiles, platforms, etc.*

2d) Overall Digital Behaviour Pattern. *Please summarise overall patterns including how much time is spent online daily, any peak usage times and levels of supervision*.

3. Vulnerability and Risk Factors

3a) Online risks identified. *Based on section 2, please provide a summary of online risks identified.*

Platform(s) involved:	
Type of risk (Content/ Contact/	

Conduct/ Commerce):	
Description of concern:	

3b) Vulnerabilities. *Please identify any additional abilities which increase might the online risk to the child.*

- ☐ Neurodivergent traits
- ☐ Domestic abuse exposure
- ☐ Poverty/digital exclusion
- ☐ Sexual or criminal exploitation
- ☐ Child looked after
- ☐ Mental health needs
- ☐ Communication / SEND needs
- ☐ Other

3c) Details of vulnerabilities

3d) How do these vulnerabilities affect online behaviour: *Please refer to LSCP Multiagency Practice Guidance: Online Safety, Section 7 and Appendix A for further support.*

3e) Main risks observed: *Please refer to LSCP Multiagency Practice Guidance: Online Safety, Section 3 for further information.*

Content risks:	
Contact risks:	
Conduct risks:	
Commerce risks:	

3f) Are there any digital neglect concerns? *Please refer to LSCP Multiagency Practice Guidance: Online Safety, Section 2.3 for an understanding of digital neglect.*

- ☐ Yes
- ☐ No
- ☐ Suspected

3g) Details of digital neglect concerns:

4. Risk Assessment

4a) How do these vulnerabilities interact to create compound risks: *For example, a neurodivergent child might have traits of impulsivity and literal thinking, which causes them to immediately accept requests from unknown users claiming to be a friend. Please refer to LSCP Multiagency Practice Guidance: Online Safety, Section 7 and Appendix A for further support.*

4b) Protective factors present:

Family support:	
Professional support:	
Digital skills:	
Other:	

4c) Overall Risk Assessment Level:

☐ Low
☐ Medium
☐ High
☐ Critical

4d) Rationale:

4e) Immediate safety concerns:

☐ Yes
☐ No

4f) Details:

5. Action Planning

5a) Actions required:

Immediate safety measures:	
Referrals needed: ☐ Social Care ☐ Police ☐ Health/CAMHS ☐ Education	

☐ Other	
Digital safety planning:	
Family/carer involvement:	

5b) Vulnerability-specific interventions required? *Please refer to LSCP Multiagency Practice Guidance: Online Safety, Section 7 further guidance.*

☐ Neurodivergent-adapted
☐ Domestic abuse specialist
☐ Digital inclusion
☐ CLA-specific
☐ Mental health support
☐ Communication support

5c) Safety planning approach:

☐ Individual
☐ Family
☐ Multi-agency

5d) Key safety plan elements:

6. Review and Monitoring

6a) Safety goals. *What is the safety that you are trying to achieve. E.g. Child will no longer interact with strangers online; child will not be exposed to harmful content, etc.*

6b) Review details

Next review date:	
Review lead:	

Appendix C: Safety Planning and Intervention Tools

Universal Safety Planning Tools

Tool 1: Traffic Light System for Online Decisions

GREEN (Safe to Go):

- Talking to friends I know offline/in real life
- Using approved platforms
- Sharing photos without personal info
- Playing games with known friends
- Posting positive content
- Asking for help when unsure

AMBER (Stop and Think)

- New friend request (Is it someone I know? Is it someone I want to connect with?)
- Someone asking personal questions
- Invitation to meet offline
- Request for photos or personal information
- Feeling upset and wanting to post immediately

RED (Stop – Get Help):

- Someone asking for private information (address, school, phone number, DoB)
- Requests for money, gifts or favours
- Threats, bullying or harassment
- Sexual conversations or requests
- Feeling scared, uncomfortable or confused

My trusted adults are:

- _____
- _____
- _____

Tool 2: STOP-THINK-CHECK-POST

Visual Reminder Card:

🛑 STOP
Before I share anything online

🤔 THINK
- Would I feel comfortable showing this to [trusted adult]?
- Does this include personal information I should keep private?
- How might others react to this?

✅ CHECK
- Privacy settings on?
- No location visible?
- No personal information visible?
- Nothing inappropriate in the background?
- Am I feeling calm and thinking clearly?

📱 POST
Only if all checks passed

Tool 3: My Personal Online Safety Rules

For [Child's Name]

1. I only accept friend requests from people I know offline/in real life
2. I never share my: _____ (address, school, name, phone number, full name, birthday)
3. If someone makes me feel uncomfortable online, I tell [trusted adult]
4. I use privacy settings on all my accounts
5. I never arrange to meet online friends without [trusted adult] knowing
6. I remember: if something seems to good to be true, it probably is

My trusted adults are:

- _____
- _____
- _____

Tool 4: Feeling Wheel for Online Emotions

When I feel … I will …

- Angry → Step away from device, use calm down strategy
- Sad → Talk to trusted adult before posting
- Excited → Use STOP-THINK-CHECK-POST before sharing news
- Lonely → Message approved friend or family member
- Confused → Ask trusted adult for help

My calm-down strategies:

- _____
- _____
- _____

Tool 5: Safety Planning for Difficult Situations

If I'm Being Bullied Online:
1. Don't respond to the bully
2. Screenshot/save evidence
3. Block and report the person
4. Tell my trusted adult immediately
5. Remember: this is not my fault

If Someone Asks to Meet Me:
1. Never agree to meet without telling my trusted adult
2. If I want to meet someone, my trusted adult must:
    - Know who, when, where
    - Be involved in planning
    - Meet the person first (if applicable)
3. Always meet in public places with my trusted adult present

If I See Upsetting Content:
1. Stop looking at it immediately
2. Tell my trusted adult
3. Use reporting tools if available
4. Do self-care activities to feel better
5. Remember: I can get help to block this content

If My Account Gets Hacked:
1. Tell my trusted adult immediately
2. Change passwords with help
3. Check what information was accessed
4. Report to platform
5. Review privacy settings together with my trusted adult

Crisis Safety Planning (When I'm Having a Really Hard Time)

Warning signs that I need extra support:
- _____
- _____
- _____

Safe online activities during difficult times:
- _____
- _____
- _____

People I can contact for support:
- **Immediate support:** _____
- **Crisis support:** _____
- **Professional support:** _____

Websites/apps that make me feel better:

- _____
- _____
- _____

Websites/apps to avoid when struggling:

- _____
- _____
- _____

Emergency Contact

If I'm in immediate danger: 999

For online safety concerns:

- **Childline:** 0800 1111 or www.childline.org.uk
- **CEOP:** www.ceop.police.uk
- **Report harmful content:** Use platform reporting or www.iwf.org.uk

My local support contacts:

- _____
- _____

Adaption Notes for Professionals

Making Tools Accessible for Different Needs:

For children with communication needs:
- Use pictures/symbols alongside text
- Provide in appropriate languages
- Use larger fonts/clear formatting
- Offer audio versions

For children with learning differences:
- Break information into smaller steps
- Use visual prompts and reminders
- Practice tools together regularly
- Create physical reminder cards

For children in crisis situations:
- Ensure tools can be used discretely
- Provide alternative communication methods
- Include safety considerations for sharing plans
- Build in multiple backup options

For children with limited resources:
- Focus on free safety options
- Include public access considerations
- Provide alternatives that don't require premium features
- Consider offline backup strategies

Tool Customisation Guidelines:

1. **Start with universal tools** and adapt as needed
2. **Involve the child** in personalizing their safety plan
3. **Regular review** to ensure tools remain relevant
4. **Consider cultural sensitivity** in language and examples used
5. **Make age-appropriate** adjustments to complexity and format
6. **Make multiple formats** available (visual, audio, text, digital, physical)

Remember: These tools should be personalized for each child's specific vulnerabilities, capabilities, and circumstances while maintaining their core safety functions.

Appendix D: Professional Practice and Supervision Guides

Essential Supervision Questions for Complex Cases

For Any Vulnerable Child:

Understanding the Child:
1. What vulnerabilities does this child have and how do they interact?
2. What needs are being met through their online behaviour?
3. What protective factors are present in their life?

Checking Our Response:
1. Are we addressing all their vulnerabilities or just focusing on one?
2. Is our approach realistic for their specific circumstances?
3. Are we building on their strengths and preserving beneficial connections?

Multi-Agency Coordination:
1. Does everyone involved understand this child's full vulnerability profile?
2. Are our interventions coordinated or potentially conflicting?
3. Who is taking the lead on each aspect of support?

Learning:
1. What is this case teaching us about intersectional vulnerabilities?
2. What would we do differently if we encountered a similar case?

Managing Professional Anxiety

When Cases Feel Overwhelming:

Practical Strategies:
- **Name the complexity:** "This child has multiple vulnerabilities that interact"
- **Share responsibility:** Ensure multi-agency team carries the load together
- **Focus on small wins:** Identify achievable changes rather than trying to fix everything
- **Access consultation:** Use specialist input when needed

Self-Care Essentials:
- **Limit exposure:** Don't spend all day on disturbing online content
- **Use supervision:** Don't carry concerns alone
- **Take breaks:** Step away from screens and cases regularly
- **Access support:** Use employee assistance programs when needed

Remember: Professional practice in vulnerability-informed online safety requires ongoing learning, regular supervision, and sustained attention to practitioner wellbeing. This is complex work that no one should do alone.

Appendix E: Glossary of Terms

4 Cs: The UKCIS model categorising online risks - Content, Contact, Conduct, Commerce

BSL: British Sign Language - used by deaf and hearing-impaired communities

CAMHS: Child and Adolescent Mental Health Services - NHS services providing mental health support for children

Care Experience: Having been looked after by local authorities at any point, including current looked-after children, care leavers, and those who have experienced kinship care or residential placements

CEOP: Child Exploitation and Online Protection Command (part of National Crime Agency)

CLA: children who are looked after - children currently in the care of local authorities

Coercive Control: Pattern of controlling, threatening, or intimidating behaviour (including through technology)

Cyberbullying: Bullying using electronic communication and digital platforms

Deepfake: Digitally altered video/image created using AI to misrepresent someone

Digital Exclusion: Lack of access to digital technologies due to financial, geographic, or other barriers including inability to afford devices, internet access, or digital literacy skills

Digital Footprint: Trail of data left by online activities and digital interactions

Digital Neglect: Failure to meet a child's online safety and wellbeing needs

Digital Self-Harm: Deliberately posting harmful content about oneself or seeking distressing content

DSL: Designated Safeguarding Lead

Grooming: Building a relationship to manipulate, exploit and abuse

Intersectional Vulnerability: When multiple vulnerability factors combine to create compound risks

LSCP: Lambeth Safeguarding Children Partnership

MARAC: Multi-Agency Risk Assessment Conference

MASH: Multi-Agency Safeguarding Hub - central point for processing safeguarding referrals and coordinating multi-agency responses

Multi-Agency: Involving professionals from different services (social care, health, police, education, etc.) working together to support children and families

Neurodivergent: People whose brains function differently from what is considered typical (includes ADHD, autism, learning differences, etc.)

NRM: National Referral Mechanism (for modern slavery/trafficking)

Phishing: Fraudulent attempt to obtain sensitive information online

Radicalisation: The process by which a person comes to support terrorism or forms of extremism leading to terrorism

SEND: Special Educational Needs and Disabilities - children requiring additional support due to learning difficulties or disabilities

Sextortion: Sexual exploitation involving threats, coercion or blackmail using digital means

Sharing nudes and semi-nudes: Self-generated sexual imagery (previously called 'sexting')

Technology-Facilitated Abuse: Use of technology to monitor, control, threaten, or harm others

Trauma-Informed: Approach that recognizes and responds to the impact of traumatic experiences on behaviour and development

UKCIS: UK Council for Internet Safety

Vulnerability-Informed Practice: Adapting approaches to account for specific vulnerability factors and their intersections