Lambeth
Safeguarding
Children
Partnership

LSCP 7-Minute Briefing: Protecting Children from Online Risk

Dec 2025

Notice: this briefing is intended to summarise and serve as a quick reference point to the LSCP Online Safety Multiagency Policy ("the Policy") and LSCP Online Safety Multiagency Practice Guidance ("the Guidance"). It does not replace or supersede the full documents, which should be referenced for further detail and full guidance.

What is online risk? Online risk refers to the dangers or threats children face when using the internet. Like technology itself, the risks are diverse, evolving and often hidden. Lambeth adopts the UK Council for Internet Safety model of 4 Cs, which categorises online risk into 4 interlinked areas

Content risk:

- What the child sees or is exposed to. E.g. pornography, hate speech, pro-suicide content, etc.

Contact risk:

- Who the child interacts with. E.g. online grooming, sexual exploitation, radicalisation, etc.

Conduct risk:

- How the child behaves online. E.g. cyberbullying, self-generated sexual imagery, etc.

Commerce risk:

- Risks relating to money and personal data. E.g. online scams, gambling-like features, etc.

How can children be exposed to online risk? Children can be exposed to online risk whenever and however they connect to the internet. Some things to consider:

- Children might use a range of **devices** to connect to the internet, for example: a smartphone, tablet, laptop or games consoles;
- Children might connect to a range of **platforms** when using the internet, for example: social media platforms (TikTok, SnapChat, Instagram, etc.), gaming platforms (Roblox, Fortnite, Minecraft, etc.), messaging platforms (WhatsApp, Discord, Telegram, etc.) or video sharing platforms (YouTube, etc.);
- Children might connect to the internet from a range of **places**, for example: their home, their school, their journey to/from school and other places that they spend their time;
- Children might connect to the internet at a range of **times**, including times when they would be expected to be asleep or in school.

If a child's online safety and wellbeing needs are not met, including lack of supervision, guidance or protection in digital environments, this is a form of neglect known as **digital neglect**.

Why does online risk matter? Online risk can cause real-world harm. This might include:

- Impaired health and development, for example, suffering from anxiety, depression or self-harm injury;
- Physical harm, for example, suffering physical violence in response to online behaviour or being groomed and exploited into gang activity;
- Sexual harm, for example, suffering sexual violence in response to online grooming or having sexual imagery published online;
- Financial harm, for example, losing money to an online scam.

What do I need to do about online risk? Safeguarding is everyone's responsibility and, by definition, it includes taking action to protect children from maltreatment **including online**. This means that you must be alert to the signs and indicators of online risk and know how to respond when these are identified.

You must also use technology responsibly and professionally in line with acceptable use policies. This includes never using personal devices to contact children nor using any social media accounts to contact children who are currently accessing a service or who have accessed it in the past.

What are the signs and indicators of online risk? Online safety concerns can present in different ways. For example, a child or parent might directly disclose, practitioners might be made aware of concerning content in circulation or indications may come via a child's behaviour. This might include, for example: secretive or obsessive use of devices, emotional distress after going online, talking about new online 'friends', sudden changes in views / beliefs or physical symptoms linked to screen use.

Are any children particularly vulnerable to online risk? Any child can be vulnerable to online harm and practitioners should be alert to signs of risk amongst all children. While all children deserve our attention and care, vulnerable children are at increased risk because they may see the online world as a place of sanctuary and comfort. These include children who are looked after, children who are neurodivergent, children impacted by domestic abuse, children with mental health needs, children experiencing in poverty, children with communication needs and children who have been criminally and sexually exploited.

What do I need to do if I suspect online risk? You should always follow your organisational safeguarding procedure and report to your safeguarding lead. Safeguarding leads and lead professionals should complete the **online safety risk assessment** template when online safety risks are suspected or disclosed. For children with additional vulnerabilities, specific attention will need to be given in assessment as to how traits of their vulnerability can manifest online.

How should I respond to online risk once identified? All responses need to be **realistic**: it is not realistic to expect a child will not connect to the internet. In specific situations, such as self-generated sexual imagery or online radicalisation, there are additional considerations like trying to remove the content and the Prevent Duty which will need to be addressed. For children with specific vulnerabilities, further consideration should be given to vulnerability-informed interventions. It is also important to consider language – for example, replacing 'attention seeking' with 'connection seeking'.

What if I am a manager or safeguarding lead who is providing consultation or supervision for a child where there is an online risk concern? Online risk can be a complex area of practice, and it is important that supervision provides a space for reflection and demonstrates professional curiosity regarding online risk and that safeguarding supervisors are equipped to ask probing and reflective questions.

What if I am a leader or involved in the strategic response to online risk? You should ensure that the specific and collective responsibilities outlined in the Policy are adapted within your own organisation. This includes ensuring that safeguarding policy and procedure gives sufficient recognition and understanding of online risk, that staff and volunteers are equipped to recognise and respond to this risk, that the online safety risk assessment template is embedded in practice and that practitioners are given clear expectations of acceptable digital behaviour.

Further resources:

- LSCP Multiagency Policy: Online Safety
- LSCP Multiagency Practice Guidance: Online Safety