# LSCP Multiagency Policy
# Online Safety

December 2025

**This Policy 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 |
|---|---|---|---|---|
| 09/12/25 | V1 | Initial draft | G Russo | LSCP Executive Board |
| | | | | |
| | | | | |

**Intended audience**
The Policy 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

# Executive Summary

Safeguarding, by definition, includes the duty to protect children from maltreatment, including online. Learning from Local Child Safeguarding Practice Reviews has highlighted that this can be a complex and challenging area of practice in an increasingly digital world.

This Policy provides a comprehensive framework for agencies and organisations working with children and families across Lambeth.

It includes clear roles and responsibilities for multi-agency staff and organisations across Lambeth. It clearly establishes what we mean by 'online risk' and highlights the emerging and evolving nature of these risks. It identifies vulnerable children who are at increased risk of online harm and sets out how to recognise these risks.

It introduces an online safety risk assessment template to help identify, evaluate and manage online risks and is complemented by the LSCP Multiagency Practice Guidance: Online Safety to embed the use of this tool in practice.

It recognises that online risk often overlaps, interacts and compounds with other forms of abuse, neglect and exploitation and includes specific resources and tools, such as removal of online content, to help manage and respond to online risk as part of proactive and coherent multi-agency responses.

It provides guidance about safe use of technology by multi-agency staff, including conduct and contact with children online and sets out clear expectations of acceptable digital behaviour.

It aims to ensure that the multi-agency workforce in Lambeth is able to effectively respond to online risk and support children's safe engagement with the online world.

All partners are expected to implement this policy within their services and contribute to Lambeth's collective commitment to digital safeguarding.

# 1. Introduction

## 1.1 Purpose of this policy

The purpose of this Safeguarding Children Online Policy is to provide clear and consistent expectations for practitioners and agencies regarding the identification, prevention and response to online harm in addition to modelling safe, respectful and appropriate digital behaviour.

In an increasingly digital world, online environments form a significant part of daily life. While digital tools offer connection, education and opportunity, they also present serious risks. These include exposure to harmful content, online grooming and exploitation, misinformation, coercive contact and various forms of digital abuse.

Online risk frequently overlaps, interacts with and compounds other categories of child abuse, neglect and exploitation. In practice, children who experience online harm often experience other forms of harm which require a proactive, coherent and comprehensive multi-agency response. This policy outlines the specific approaches which should be used to respond to online risk and must be adopted alongside existing policy, procedure and guidance which outlines how all forms of abuse, neglect and exploitation must be responded to.

This policy outlines Lambeth's collective commitment to protecting all children – especially those most vulnerable – from online harm, by embedding robust online safety measures across all services. It also sets out shared expectations for safe and appropriate professional conduct when engaging with digital tools or working with people online.

The policy compliments and integrates with existing Lambeth safeguarding frameworks and should be read alongside the LSCP Multiagency Practice Guidance: Online Safety.

## 1.2 Scope of policy

This policy applies to all multi-agency staff who work within agencies and organisations with functions relating to children living in, or looked after by, Lambeth and their families. This includes (but is not limited to):

- Lambeth Council staff
- Education and early years settings
- Youth and family services
- Health professionals (e.g. NHS trusts, Mental Health Trusts, Primary Care)
- Police and community safety teams
- Voluntary and community sector organisations
- Commissioned providers and contracted services
- Private fostering arrangements
- Secure children's homes and residential settings

This policy is relevant to any context in which children engage with digital technologies, including, but not limited to, websites, social media platforms, messaging apps, livestreaming services, gaming platforms, AI-based tools and virtual learning environments. This policy is also relevant to the digital behaviour of multi-agency staff in discharging their roles and responsibilities.

## 1.3 Definitions

For the purpose of this policy, the following terms are defined as:

- **Children**: all individuals aged under 18.
- **Online Safety:** 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:** Any abuse, exploitation or psychological harm experienced via online platforms or digital interactions.
- **Multi-Agency Staff:** Any professionals or volunteers working across different sectors in a collaborative safeguarding role, including statutory, voluntary and community services.
- **Vulnerable Children:** Children whose circumstances may increase their susceptibility to online risk or exploitation, including (but not limited to) children with SEND or mental health needs, care-experienced children and those with learning difficulties, disabilities, neurodivergent conditions or socio-economic disadvantage.
- **Digital Citizenship:** The responsible and positive use of technology, encompassing digital literacy, online ethics and active participation in digital communities.
- **Digital Neglect:** A form of neglect where a child's online safety and wellbeing needs are not met, including lack of supervision, guidance or protection in digital environments.

Further terminology is detailed in Appendix C.

## 1.4 Legal and policy framework

This policy is grounded in a comprehensive legal and statutory framework that reflects the UK's commitment to safeguarding children from harm in digital environments. All multi-agency partners in Lambeth are expected to be familiar with these frameworks and to embed them in their own practise.

Key Legislation:

- Online Safety Act 2023
- Children Act 1989 & 2004
- Education Act 2002 (Section 175/157)
- Children and Social Work Act 2017
- Data Protection Act 2018 & UK GDPR
- Equality Act 2010
- Counter-Terrorism and Security Act 2015
- Human Rights Act 1998
- Communications Act 2003
- Protection From Harassment Act 1997

- Voyeurism Offences Act 2019
- Domestic Abuse Act 2021

Statutory Guidance and National Policy:
- Working Together to Safeguard Children 2023
- Keeping Children Safe in Education (KCSIE) 2025
- DfE Guidance: Teaching Online Safety in Schools (updated 2023)
- UK Council for Internet Safety (UKCIS) Frameworks
  - Education for a Connected World Framework
  - Online Safety in Education Settings: Guidance for DSLs
  - Sharing nudes and semi-nudes: advice for education settings
- Prevent Duty Guidance (2023)
- ICO Guidance on Children's Privacy Online

Local Alignment and Multi-Agency Expectations - this policy aligns with and complements:
- Lambeth's Multi-Agency Arrangements to Safeguard Children (Dec 2024)
- London Safeguarding Children Procedures
- Pan London Threshold Document: Continuum of Help and Support
- Lambeth Children's Services Procedures Manual
- Lambeth Children's Services Domestic Abuse Policy
- Lambeth Multi-Agency Neglect Strategy and Toolkit
- Local Information Sharing Agreements
- Commissioning standards for online services
- Lambeth Multi-Agency Escalation Pathway
- Lambeth Serious Incident Notification procedures
- The London Child Exploitation Operating Protocol 2021 and the DRAFT London Multi Agency Child Exploitation and Harm Outside the Home Protocol – 5th Edition

All partners are expected to use this framework to review their own policies and ensure consistency with national expectations and Lambeth's local safeguarding arrangements.

## 1.5 Civil Orders

Multi-agency staff should be aware of available civil orders that can provide protection from online harm:
- Sexual Risk Orders (SROs) can prohibit individuals from specific online activities
- Sexual Harm Prevention Orders (SHPOs) include restrictions on internet use
- Restraining Orders can include provisions about online contact
- Non-Molestation Orders cover digital harassment and abuse
- Domestic Violence Protection Orders can include technology-related restrictions

# 2. Aims and principles

## 2.1 Policy aims and objectives

The overarching aim of this policy is to ensure that all children in Lambeth are protected from online harm and empowered to use digital technologies safely and positively.

Specifically, this policy seeks to:

- Establish a consistent, multi-agency approach to identifying, preventing and responding to online safety concerns.
- Embed online safeguarding within wider safeguarding practises, recognising digital risk as an integral part of safeguarding in society today.
- Promote digital resilience and positive digital citizenship among children, families and the multi-agency staff who support them.
- Raise awareness of the nature and scope of online risks, including evolving harms such as AI-generated abuse, live streaming and targeted grooming.
- Support multi-agency staff in making confident, proportionate decisions when responding to online safety issues.
- Strengthen professional conduct and digital responsibility in the way multi-agency staff use technology in their work with children.
- Support Lambeth's commitment to addressing the specific needs of groups facing particular vulnerabilities online.

## 2.2 Principles

This policy is guided by the following core principles, reflecting both statutory duties and shared values across Lambeth's safeguarding partnerships:

- **Safeguarding is Everyone's Responsibility – Including Online** Every professional and volunteer who works with or on behalf of children has a duty to understand online risks and respond appropriately.
- **Children's Rights are Central** This policy upholds children's rights as set out in the United Nations Convention on the Rights of the Child (UNCRC), including:
    - The right to be protected from violence, abuse and neglect (Article 19)
    - The right to privacy and protection of personal data (Article 16)
    - The right to information and participation (Articles 12, 13 and 17)
    - Children must be included in shaping online safety approaches, and their views must be heard and acted upon.
- **Prevention is Better than Reaction** Online risks often escalate quickly and are hidden from parents, responsible adults and multi-agency staff until harm occurs. Early identification, prevention and proactive digital education are key. This includes strengthening families' capacity to support their children and equipping professionals to spot early signs of concern, including digital neglect.
- **Equity and Inclusion are Essential** Certain individuals and communities face greater risk online due to systemic barriers, unmet needs or intersecting vulnerabilities. Online safety

responses must be inclusive, accessible, vulnerability-informed and trauma-informed, with particular attention paid to those most at risk of being unseen or misunderstood.

- **Technology Is Not Neutral** Digital platforms are designed with commercial, behavioural and social drivers that can amplify risk. Multi-agency staff must understand how design, algorithms and platform culture influence harm, and they must work with families and young people to build awareness and critical thinking.
- **Working Together is Vital** No single agency can keep children safe online. Effective safeguarding requires joined-up working, shared information and clarity of thresholds as set out in the Pan-London Threshold Document. Multi-agency teams must collaborate to provide a coordinated and confident response.
- **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** Multi-agency staff 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. Roles and responsibilities

Online safety is a shared safeguarding responsibility. All individuals working with or on behalf of children in Lambeth have a duty to understand online risks and take appropriate action to prevent harm. This includes staff in all statutory services, commissioned partners and voluntary sector organisations.

To ensure a robust, joined-up response, this section sets out the specific and collective responsibilities of multi-agency professionals, aligned with Lambeth's Multi-Agency Arrangements to Safeguard Children.

Practice guidance to help discharges these responsibilities is available in the LSCP Multiagency Practice Guidance: Online Safety.

## 3.1 Lambeth Local Authority

Lambeth Council, as the lead safeguarding agency, holds strategic responsibility for ensuring that effective online safety measures are in place across all relevant services working with children.

Key responsibilities include:

- Ensuring that all council-run and commissioned services have online safety policies aligned with this framework.
- Leading coordinated local response to emerging or complex digital safeguarding concerns.
- Monitoring compliance with relevant legislation (e.g. Online Safety Act 2023, Data Protection Act 2018).

- Ensuring online safety is integrated into school safeguarding checklists (S175s).
- Allocating appropriate resources and funding for online safety initiatives.
- Maintaining Service Level Agreements (SLAs) with partner agencies.

## 3.2 LSCP governance and online safety oversight

Online safety is overseen through the LSCP governance structure, which includes:

**Strategic Level:**
- The LSCP Executive Board provides strategic oversight of online safety as part of its broader safeguarding responsibilities.
- The Quarterly Safeguarding Assurance Group reviews high-level online safety challenges and risks.
- The Strategic Risk Outside the Home meeting (MAROTH) monitors the effectiveness of mult-agency safeguarding responses to risk outside the home.

**Operational Level:**
- The Performance, Challenge and Impact Subgroup monitors online safety data and outcomes and ensures online safety is integrated within section 11 audits.
- The Contextual Safeguarding Strategic Oversight Group addresses online risks as part of extra-familial harm.
- The Education Safeguarding Advisory Committee (ESAC) oversees online safety in educational settings.
- The Learning & Improvement subgroup provides training and development opportunities for multi-agency staff through the LSCP training programme.
- The Multi-Agency Child Exploitation (MACE) panel provides an operational space to consider children at risk of, or already subject to, harm through exploitation.
- Thematic groups may be established for specific online safety priorities.

**Key responsibilities for online safety oversight include:**
- Reviewing policy implementation and emerging risks.
- Coordinating multi-agency responses to complex online safety cases.
- Monitoring data and trends in online harm.
- Ensuring online safety is embedded in training programmes.
- Contributing to the LSCP Annual Report.
- Implementing learning from serious case reviews and safeguarding practice reviews.
- Overseeing serious online safety incidents.

## 3.3 Safeguarding leads and named Professionals

Every organisation or service working with children must have appropriate safeguarding leadership arrangements (and where possible, a named person with specific responsibility for online safety), which may include:
- Local Authorities:
  - Services Managers, Assistant Directors and Directors.

- Education Settings:
  - Designated Safeguarding Lead (DSL) and Deputy DSL(s).
  - Named person with specific responsibility for online safety where possible.
- Health Services:
  - Named safeguarding professionals (doctors, nurses, midwives).
  - Links to strategic designated safeguarding professionals at ICB level.
- Police:
  - Public Protection Units
- Other Agencies:
  - Named safeguarding leads or managers.
  - Designated online safety champions where appropriate.

Key responsibilities for operational safeguarding leads include:

- Leading on all online safety concerns, referrals and risk assessments.
- Staying up to date with local and national developments in digital safeguarding.
- Ensuring all staff receive appropriate online safety training and support aligned with LSCP requirements.
- Liaising with external agencies (e.g. police, social care, CEOP, Ofcom) where needed.
- Maintaining records and reviewing learning from digital safeguarding incidents.
- Conducting annual online safety audits within their organisation.
- Ensuring staff wellbeing when dealing with disturbing online content.
- Following the serious incident notification process for significant online safety concerns.
- Implementing the multi-agency escalation pathway when required.

## 3.4 Education and early years providers

Schools, colleges and early years settings play a critical role in identifying and responding to online harm, and in educating children about safe digital behaviour. Education is recognised as a key partner in safeguarding arrangements.

Responsibilities include:

- Embedding online safety within the PSHE/RSHE curriculum and whole-school culture.
- Following statutory guidance in Keeping Children Safe In Education (KCSIE).
- Monitoring pupils' use of digital tools on school devices and ensuring age-appropriate filtering and monitoring systems are in place.
- Ensuring IT equipment is not being used to facilitate the spread of extremist narratives which encourage people into participating in or supporting terrorism.
- Considering the use of harmful content filters on school devices as part of their overall strategy to prevent people from becoming involved in, or supporting, terrorism.
- Supporting families to understand and manage digital risks at home.
- Ensuring staff modelling of safe and respectful digital practice.
- Maintaining clear acceptable use policies for staff and students.
- Implementing digital safety plans for vulnerable pupils.
- Completing the annual Lambeth schools safeguarding checklist (s157/175 requirements).
- Identifying and responding to digital neglect as part of broader neglect concerns.

## 3.5 Children's social care and early help teams

Social care staff must routinely consider digital risk as part of their safeguarding and wellbeing assessments, aligned with the Pan-London Threshold Document.

Responsibilities include:

- Identifying online harms and abuse (e.g. grooming, image-based abuse, coercive control) during assessments and planning.
- Recognising digital neglect as a form of neglect requiring intervention.
- Providing children and families with guidance and support around safe technological use.
- Liaising with specialist agencies where digital exploitation is suspected.
- Incorporating digital safety into child protection, CIN and early help plans.
- Developing appropriate digital safety plans.
- Ensuring transitions to adult services include online safety considerations.
- Coordinating responses for missing children who may be at risk online.

## 3.6 Health professionals

Health services, including Primary Care, Mental Health Trusts, CAMHS, A&E and school nurses, play an essential role in recognising the impact of online harm on mental, emotional and physical health.

Responsibilities include:

- Including questions about digital life and screen use in assessments.
- Identifying signs of digital trauma, self-harm or exposure to harmful online content.
- Ensuring IT equipment managed by the service is not being used to facilitate the spread of extremist narratives used to encourage people into participating in or supporting terrorism.
- Considering whether IT equipment available to the public should use filtering solutions that stop access to material which supports terrorism or extremist ideas linked to terrorism.
- Working collaboratively with families, education and social care on safeguarding plans.
- Signposting to appropriate services, including mental health and safety resources.
- Considering online safety in hospital admission and discharge planning.
- Supporting children to understand the health impacts of excessive screen time.

## 3.7 Police and community safety teams

The police have both a preventative and enforcement role in online safety, including investigation of online offences, collaboration with partners and proactive risk reduction.

Responsibilities include:

- Investigating online abuse, grooming, exploitation, harassment or radicalisation involving children.
- Working with CEOP, the Internet Watch Foundation and other national safeguarding partners.
- Sharing relevant intelligence with multi-agency partners to prevent harm.

- Ensuring IT equipment is not being used to facilitate the spread of extremist narratives used to encourage people into participating in or supporting terrorism.
- Supporting safety planning for children at risk of online threats.
- Providing guidance on evidence preservation and digital forensics.
- Liaising with the Crown Prosecution Service on online offence cases.
- Implementing appropriate civil orders to protect victims.
- Contributing to MARAC where technology-facilitated abuse is identified.

## 3.8 Voluntary and community sector (VCS) and commissioned providers

VCS organisations and commissioned services, including those offering mentoring, youth work and therapeutic support, are key partners in both digital safeguarding and building digital resilience.

Responsibilities include:

- Ensuring staff and volunteers are trained in online safety relevant to their roles, and that training is kept up to date.
- Implementing safe digital communication and data handling practices.
- Supporting children to understand their rights and responsibilities online.
- Recognising when online behaviours may indicate wider safeguarding concerns.
- Meeting contractual requirements for online safety as specified in SLAs.
- Contributing to multi-agency information sharing and case discussions.
- Providing culturally appropriate online safety support to diverse communities.

## 3.9 Residential and foster care providers

Those caring for children who are looked after have particular responsibilities given the vulnerabilities of this cohort.

Responsibilities include:

- Implementing appropriate supervision and support for internet use.
- Balancing safety with normal developmental needs.
- Supporting contact arrangements that may involve digital communication.
- Managing risks associated with social media and previous relationships.
- Ensuring staff are trained in online safety specific to care settings.
- Maintaining clear policies on device use and online access.
- Recognising and responding to digital neglect.

## 3.10 All staff and volunteers

Everyone working in a professional or voluntary capacity with children or vulnerable adults has a responsibility to:

- Stay informed about current and emerging online risks.
- Act in accordance with safeguarding procedures when concerns arise.
- Use technology responsibly and professionally in line with acceptable use policies.

- Support and educate children and families about digital safety.
- Report any breaches of policy or inappropriate digital conduct.
- Complete mandatory online safety training within specified timeframes.
- Consider cultural and religious factors when discussing online behaviour.
- Use the multi-agency escalation pathway when concerns are not being addressed.

### 3.11 Parents and carers

Multi-agency staff should work closely with parents and carers, recognising their vital role in keeping children safe online. Services should:

- Share accessible guidance and advice, including resources in multiple languages.
- Encourage open communication between parents/carers and children.
- Signpost to trusted resources and support services.
- Respect the diverse ways that families engage with technology.
- Address digital poverty and access issues that may increase risk.
- Support families where English is not the first language through appropriate interpretation services.

## 4. 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. Multi-agency professionals 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.

### 4.1 The 4 Cs 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.

## 4.2 Emerging and evolving risks

Online harm is consistently shifting in form and platform. Multi-agency staff 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.

## 4.3 Vulnerability factors

Some children are more at risk of online harm due to personal, social or structural vulnerabilities. These include:

- Neurodivergent children (both diagnosed and undiagnosed) who may struggle with social cues, impulsivity, rigid thinking or loneliness and isolation, making them more susceptible to grooming, exploitation or misinformation. This includes children with ADHD whose impulsivity may increase online risk-taking behaviours.
- Children with SEND particularly those with communication or cognitive needs who may find it harder to understand risk or seek help.
- Care-experienced children who may seek connection or affirmation online and be less protected by family support structures.
- Children experiencing poverty who may rely on unsafe public Wi-Fi, outdated parental controls or cheaper, riskier tech platforms.
- Children with mental health need who may be drawn to and into harmful communities or content during periods of distress.
- Children affected by trauma who may find unsafe online spaces that mirror their experiences or exploit their vulnerabilities.
- Those with limited English or digital literacy who may struggle to access safety information or understand platform controls.
- Children in residential settings who may have limited supervision or support.
- Children affected by domestic abuse who face specific risks online as identified in Lambeth research, including disproportionate exposure to online hate speech (43% compared to 37% overall, according to the Digital Youth Index 2021 report) and targeted racism that can correlate with offline harm. Digital exclusion and access barriers may also increase vulnerability in online spaces.

## 4.4 Recognising signs of online harm

Signs that a child or young person 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 (albeit this may also be as a result of wider issues, including neglect).

Multi-agency staff 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.

## 4.5 Cultural and religious considerations

When assessing online risks, multi-agency staff must be sensitive to:
- Different cultural norms around privacy, relationships and online expression.
- Religious perspectives on appropriate content and behaviour.
- Intergenerational differences in digital understanding within families.
- The potential for online spaces to be used for cultural or religious coercion.
- The importance of culturally appropriate support and intervention.
- Language barriers that may prevent families accessing safety information.
- The need for interpretation services when discussing online safety.

## 4.6 Assessing the risk in practice

When online harm is suspected or disclosed, multi-agency staff 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)?

Assessments should be multi-agency where appropriate, and include the child's own views. Immediate risks should be escalated in line with the Pan-London Threshold document and Lambeth's safeguarding procedures. Use the Online Safety Risk Assessment Template in Appendix A. The LSCP Multiagency Practice Guidance: Online Safety provides further support regarding using the risk assessment tool in practice.

## 4.7 When to use the online safety risk assessment template

The Online Safety Risk Assessment Template should be used in the following circumstances:

- When online safety risks are suspected or disclosed during any professional contact.
- When virtual non-attendance raises safeguarding concerns.
- When multiple vulnerability factors are present that increase online risk.
- When multi-agency coordination is required to address digital harm.
- When developing digital safety plans or interventions.
- When reviewing and updating existing safeguarding plans to include online safety considerations.

The template supports consistent assessment across agencies and ensures that all relevant risk factors are considered systematically.

The template does *not* replace existing risk assessment and analysis tools for responding to child abuse, neglect and exploitation; instead it aims to enhance these assessment tools by enabling enhanced reflection and analysis of the online elements of harm.

# 5. Prevention and education

Creating safe online environments require more than reacting to harm. It involves proactive, joined-up efforts to educate, support and empower children, families and professionals. Prevention is most effective when it is embedded across all services, relationships and systems in a way that is inclusive, evidence-formed and rights-respecting.

## 5.1 Embedding online safety in everyday practice

All services working with children must integrate online safety into their core safeguarding practice, including:

- Routine consideration of digital risks in assessments, care planning and interventions.
- Using everyday interactions as opportunities to model safe digital behaviour.
- Ensuring clear, safe boundaries in digital communication with children.
- Encouraging open conversations about online experiences and concerns.
- Recognising that online risk may be part of a wider pattern of harm, trauma or exploitation.
- Promoting positive digital citizenship alongside risk management.
- Integrating online safety within early help approaches.
- Considering digital neglect within the Lambeth Neglect Strategy and Toolkit.
- Knowing that a child's online life is as significant as their offline ('real' world) life.
- Considering the sequencing and timing of multiple interventions to avoid overwhelming children.
- Coordinating interventions across agencies to ensure coherent support.

## 5.2 Online safety education for children

Education is a key tool in preventing harm and empowering digital confidence. All education and youth settings should:

- Teach age-appropriate online safety content across the curriculum, especially through PSHE and RSHE.
- Consider using frameworks such as the Educated for a Connected World to build progression from early years to post-16.
- Focus on critical thinking, digital rights, respectful online behaviour and help-seeking.
- Provide interactive, inclusive resources that reflect real-life online experiences.
- Create opportunities for children to shape digital policy and peer education.
- Address intersectional risk, including issues or race, gender, sexuality, disability and neurodiversity.
- Include positive messages about digital creativity, connection and opportunity.
- Provide specific support for groups identified as at a higher risk, including neurodivergent children.
- Schools and colleges must ensure their approach reflects current statutory guidance from Keeping Children In Education (KCSIE) and the DfE's guidance on Teaching Online Safety in Schools.

## 5.3 Support for parents and carers

Parents and carers are key to building safe online environments at home. Multi-agency staff should:

- Provide families with reliable, accessible guidance on managing digital risks.
- Share trusted resources (e.g. Internet Matters, Childnet, NSPCC, and Act Early).
- Encourage non-judgmental dialogues between parents/carers and children.
- Help families understand parental controls, privacy settings and platform risks.
- Recognise that digital challenges can be more complex in families experiencing poverty, stress or language barriers.
- Address digital poverty through device lending schemes and affordable connectivity.
- Provide culturally sensitive resources and support in multiple languages.
- Offer specific guidance regarding technology for families affected by domestic abuse.

Work with parents/carers should emphasise collaboration, not control, building confidence to guide their children without shame or fear. Resources should be made available through local appropriate channels.

## 5.4 Workforce development and training

All multi-agency staff working with children should have access to regular training and development to build confidence and competence in online safety.

Agencies should ensure that Inductions for multi-agency staff include recognition of online risk and safety and that mandatory safeguarding training related to roles and responsibilities is provided in line with LSCP Training Levels.

The LSCP training programme should include specialist courses on key online safety topics based on local needs as identified from learning processes including Child Safeguarding Practice Reviews. Examples of areas that may be covered include:

- Online grooming and exploitation
- Harmful sexual behaviour online
- Online radicalisation and Prevent duty
- Digital neglect identification and response

Specific courses, duration and availability will be determined by the LSCP based on local needs and priorities. Training should be inclusive, accessible, trauma-informed and reflect the realities of frontline work. It should incorporate learning from local serious case reviews and child safeguarding practice reviews.

## 5.5 Tools and resources to support practice

Multi-agency professionals are encouraged to use a range of evidence-based tools to support prevention and education, including:

- Project Evolve**:** UKCIS-aligned resource bank for progressive online safety teaching
- CEOP Education (ThinkUKnow)**:** Age-appropriate sessions and videos for children and parents
- SWGfL 360 Safe Tool: School and setting self-assessment for digital safeguarding
- NSPCC Online Safety Hub**:** Research, guidance, and resources for professionals and families
- Internet Watch Foundation (IWF)**:** Reporting child sexual abuse content
- Internet Matters**:** Guides for families on privacy, parental controls, and platform-specific risks
- Ofcom and ICO: Regulatory guidance on platform responsibilities and children's digital rights
- LSCP Website**:** Local resources, guidance, and training information

Lambeth services should ensure multi-agency staff have access to relevant online safety resources and tools. A suggested resource list is provided in Appendix B.

## 5.6 Promoting digital resilience and positive digital citizenship

Effective prevention is not only about managing risk, but also about building the skills and confidence that enable children to thrive online.

Digital resilience includes the ability to:

- Recognise unsafe or manipulative behaviour
- Understand personal digital boundaries
- Navigate misinformation and harmful narratives
- Seek help and report concerns

- Recover and learn from negative experiences
- Use technology positively, creatively, and ethically
- Contribute to positive online communities
- Understand digital rights and responsibilities

Multi-agency staff should model and promote these skills, helping to create a culture where safety, dignity and empowerment are at the heart of digital life.

# 6. Procedures for responding to concerns

Multi-agency staff must be equipped to respond confidently and consistently when online safety concerns arise. Responses should be timely, proportionate and centred around the child. This section outlines the processes to follow when concerns are identified, disclosed, observed or reported, aligned with Lambeth's Multi-Agency Arrangements to Safeguard Children.

## 6.1 Recognising and responding to online concerns

Online safety concerns may present in a number of 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.

When any concern arises:

- Always take the concern seriously.
- Remain calm and non-judgmental.
- Do not attempt to investigate or access devices without appropriate consent or authority.
- Reassure the child and clarify that you may need to share the concern for their safety.
- Record the concern clearly.
- Report immediately in line with your organisation's safeguarding procedures.
- Consider immediate safety and whether emergency services are needed.
- Follow the serious incident notification process if required.

## 6.2 Escalation and referral pathways

Where the concern indicates potential harm or risk of harm, the following steps should be taken:

- **Education Settings:** Report to the Designated Safeguarding Lead (DSL) or Deputy Safeguarding Lead who will assess the need for referral.
- **Health Services:** Follow organisational safeguarding procedures.

- **Other Agencies:** Follow your setting's safeguarding procedures and report to your named safeguarding lead or manager.

## 6.3 Specific online risk scenarios

Some online concerns require tailored responses. Multi-agency staff 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 and/or make a direct children social care referral 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 and refer accordingly.
  - Use the LSCP Neglect Toolkit to assess.
  - 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, directly or via discussion with colleagues 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.

## 6.4 Removal of harmful online content

Where there is harmful content of a child online, multi-agency staff 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.

## 6.5 Working with police and statutory agencies

When involving police or statutory partners:

- Share only necessary, proportionate information in line with UK GDPR and safeguarding protocols.
- Where devices may contain evidence, do NOT access, delete or forward content.
- Maintain clear records of what was reported, when and to whom.
- Support the child throughout any investigative process and ensure they are aware of next steps.

- Ensure appropriate adults are present for any interviews.
- Consider use of intermediaries where communication needs exist (e.g. if the child has SEND, has communication difficulties due to being neurodivergent or due to English not being their first language).

## 6.6 Recording, monitoring and review

All online safety concerns must be recorded securely in line with your organisation's safeguarding recording procedures.

Records should include:

- A factual account of what was disclosed, observed or suspected.
- Platforms and accounts used by both victim and perpetrator (where known).
- Action taken, including advice sought and referrals made.
- Names and contact details of any agencies involved.
- Any ongoing risk assessments or support plans.
- Evidence of content removal attempts and outcomes.
- Review dates and outcomes.
- Steps taken to preserve digital evidence (e.g. securing devices, photographing screens).
- Links to other safeguarding concerns (e.g. neglect, domestic abuse).

Safeguarding leads should review online safety incidents quarterly to identify patterns, training needs or emerging risks within the organisation or across services. This date should contribute to:

- LSCP quarterly reporting processes.
- Annual safeguarding reports.
- Section 11 audits.
- Schools safeguarding checklist returns (linked to s157/175 requirements).

## 6.7 Supporting the child

After responding to a concern, multi-agency staff should ensure that:

- The child is emotionally supported, and their voice is central in any response plan.
- Safety planning includes online risks (e.g. blocking contacts, privacy settings, supervised access).
- They are aware of their rights, how to seek help again and who they can talk to.
- Families are involved where safe and appropriate, and given guidance to manage the situation.
- Signposting is provided to therapeutic services, advocacy or support resources.
- Cultural and communication needs are addresses, including interpretation services.
- Follow-up support is planned and delivered.
- Links are made to other relevant support (e.g. domestic abuse services, Prevent support).
- A trauma-informed, compassionate approach is essential, particularly when online harm has caused shame, fear or long-term emotional impact.

## 6.8 Virtual appointments and digital service delivery

When children are not brought to virtual appointments that they are expected to attend:

- Recognise this as a potential safeguarding concern.
- Follow the standard "Was Not Brought" guidance, considering how these apply to virtual appointments.
- Consider barriers to engagement (digital poverty, language, anxiety).
- Assess whether non-attendance indicates wider concerns which need to be investigated or flagged to other agencies. Where online risks are identified, consider using the Online Safety Risk Assessment Template (Appendix A) to systematically assess and document concerns.
- Document patterns and escalate if necessary.

# 7. Safe use of technology by multiagency staff

Multi-agency staff working with children have a responsibility to model safe, respectful and appropriate digital behaviour. The way technology is used by them, including communication, record-keeping and digital service delivery, must uphold safeguarding principles and reflect the values of care, professionalism and accountability.

## 7.1 Digital professionalism

All multi-agency staff must:

- Maintain clear professional boundaries when using digital technology.
- Use organisational platforms, devices and emails for work-related communication.
- Never use personal devices or social media accounts for contacting children or their families who are currently accessing their service or have accessed their service in the past.
- Communicate using secure, approved platforms (e.g. encrypted email, case management systems or designated messaging apps).
- Consider the power dynamics involved in online contact, especially with children.
- Challenge and report any inappropriate use of technology by colleagues or service users.
- Be aware of their digital footprint and how it may impact their professional role.
- Follow guidance on working with interpreters in digital contexts.
- Professionals and volunteers should never 'friend', follow or engage with children on personal social media accounts.

## 7.2 Online meetings and virtual services

Where digital communication or virtual services are used (e.g. online therapy, remote teaching, virtual reviews), the following guidance applies:

- Use only approved platforms that meet organisational and data protection standards.
- Ensure appropriate privacy settings, waiting rooms and screen sharing controls are in place.
- Maintain a professional environment, including dress, background and conduct.
- Obtain informed consent where appropriate for digital sessions, including for children under 13 (with parental consent).

- Avoid one-to-one video calls with children unless explicitly agreed and risk-assessed.
- Record any safeguarding concerns or incidents that arise during digital sessions and escalate as needed.
- Be mindful of the potential for digital fatigue, distress or disengagement, especially with neurodivergent or vulnerable children.
- Consider accessibility needs (BSL interpreters, screen readers etc).
- Have contingency plans for technical failures.
- Monitor attendance patterns as potential safeguarding indicators.

## 7.3 Social media use by multi-agency staff

Multi-agency staff are entitled to use personal social media but must do so in a way that:

- Does not compromise their professional role.
- Does not breach confidentiality or bring their organisation into disrepute.
- Respects the privacy and dignity of children.
- Does not engage in any conduct that could be viewed as discriminatory, abusive or unsafe.
- Maintains proper privacy settings.
- Avoids discussing work-related matters.
- Does not target or refence specific vulnerable groups inappropriately.

When multi-agency staff use professional social media (e.g. public profiles for education, advocacy or outreach) they must:

- Adhere to their organisation's social media policy.
- Avoid posting or sharing identifiable information about children.
- Use respectful, inclusive and accessible language.
- Signpost only to approved resources.
- Maintain separate professional and personal accounts.
- Seek approval for content where required or if they are unsure about something.

## 7.4 Use of personal devices

Many multi-agency staff now use mobile phones, tablets or laptops to support their work. Organisations must have clear guidance on:

- Whether and when personal devices may be used.
- Secure handling of information, including encrypted apps and device passcodes.
- Avoiding the use of personal cameras, storage or messaging platforms.
- Ensuring that sensitive data is not downloaded or stored locally on personal devices.
- Insurance and liability considerations.
- Remote wiping in case of loss or theft.

Where personal devices use is permitted, it should be risk-assessed, time-limited and subject to monitoring.

## 7.5 Cybersecurity expectations

Multi-agency must adhere to basic cybersecurity practices, including:

- Using strong, unique passwords and updating them regularly.
- Never sharing login details or leaving devices unattended and unlocked.
- Reporting suspected phishing attempts, malware or data breaches immediately.
- Completing mandatory cybersecurity and data protection training.
- Ensuring organisational software and systems are kept up-to-date and secure.
- Using two-factor authentication where available.
- Being aware of social engineering tactics.

Organisations should support staff by maintaining clear ICT policies, two-factor authentication and secure data sharing systems.

## 7.6 Staff wellbeing and exposure to harmful content

Recognising that multi-agency staff may be exposed to disturbing contents, organisations should:

- Provide access to supervision and support.
- Offer employee assistance programmes including counselling.
- Rotate duties where possible to limit exposure.
- Ensure staff and volunteers know how to report secondary trauma.
- Provide guidance on self-care strategies.
- Consider impact on workload in planning.
- Provide specific support following serious incidents.

## 7.7 Breaches and misuse

Breaches of safe technology use by multi-agency staff may result in:

- Internal disciplinary action, depending on the nature of the breach.
- Referral to statutory safeguarding or regulatory bodies, such as the LADO, where concerns involve potential harm to children.
- In serious cases, police involvement or referral to professional regulators appropriate to the staff member's role.
- Review of training needs and support systems.

All concerns about digital conduct should be taken seriously, recorded and investigated in line with safeguarding and HR procedures.

# 8. Data protection and information security

The responsible use of digital technologies must go hand in hand with the secure handling of personal information. Children have the right to privacy and to expect that their personal data will be handled safely, fairly and lawfully. In the context of online safeguarding, these obligations are even more critical.

## 8.1 Legal and regulatory framework

All data handling must comply with the following UK legislation and guidance:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Children Act 1989 & 2004 (in relation to information sharing for safeguarding)
- Working Together to Safeguard Children (2023)
- Information Commissioner's Office (ICO) guidance, especially on children's data and digital services.
- Online Safety Act 2023, including transparency requirements for platforms and user data management.

These frameworks establish that data must be:

- Processed lawfully, fairly, and transparently.
- Collected for specified and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Stored securely and for no longer than necessary.

## 8.2 Sharing information for safeguarding purposes

Information sharing between multi-agency staff is essential to safeguard and promote the welfare of children. The fear of breaching data protection laws must never be a barrier to doing what is legally and ethically right in a safeguarding context.

Multi-agency staff must:

- Share information on a need-to-know basis.
- Ensure that it is proportionate, relevant and accurate.
- Record the rationale for sharing, or not sharing, sensitive information.
- Use secure channels (e.g. encrypted emails, password-protected files).
- Follow London Safeguarding Procedures information sharing protocols.
- Involve the child and their family where appropriate, unless doing so would increase risk.
- Be aware of required timescales for sharing, especially for urgent concerns.

When urgent safeguarding concerns arise, data protection should not be used as an excuse to withhold potentially life-saving information.

## 8.3 Safe storage and transfer of information

All digital records and communications must be stored and transferred in accordance with organisational policies and best practice:

- Use organisational systems (e.g. approved case management tools, secure drives).
- Avoid saving information on personal or unencrypted devices.
- Ensure devices are protected by strong passwords and time-out locks.

- Back up records in line with data retention and business continuity plans.
- Ensure that paper-based records of digital harm (e.g. transcripts, screenshots) are stored securely and cross-referenced digitally.
- Follow organisational data retention policies.

## 8.4 Digital consent and online communications

Multi-agency staff must be clear about when and how informed consent is required in digital contexts, especially when working with children and families.

- Children under 13 cannot legally give consent to data processing for most online services – parental consent is required.
- Where services are delivered online (e.g. virtual therapy, support sessions), consent for participation and data use must be obtained and recorded.
- Clear information must be provided in accessible formats, especially for those with learning disabilities, language barriers or neurodiversity.
- Consider Gillick Competence for children under the age of 16.
- Ensure interpretation services are used where needed.

## 8.5 Handling digital images and recordings

Using images, videos or recordings in a professional capacity (e.g. for case records, promotional materials, training or online engagement) must be approached with caution and care.

Multi-agency staff must:

- Always obtain informed consent before capturing or using digital images.
- Be clear about the purpose, storage and duration of use.
- Avoid taking or storing images on personal devices.
- Never share images of children on social media without specific written consent.
- Follow organisational procedures on the secure storage, encryption and deletion of media files.
- Ensure that any use of images is dignified, respectful and non-exploitative.
- Be aware of additional sensitivities around looked-after children.
- Consider specific risks for certain groups (e.g. children at risk of exploitation).

## 8.6 Responding to breaches and concerns

If a data protection beach is suspected or confirmed:

- Report immediately to your organisation's Data Protection Officer or designated lead.
- Record what happened, when and what actions were taken.
- Follow internal incident management and breach notification protocols.
- If the breach poses a risk to the child or young person's rights or welfare, consider whether to:
    - Notify the Information Commissioner's Office (ICO).
    - Inform the child and/or parent/carer where appropriate.

  - Make a safeguarding referral if the breach reveals risk or harm.
- Consider serious incident notification requirements.

All staff must complete mandatory data protection training aligned with LSCP requirements and understand their responsibilities under UK GDPR and safeguarding law.

### 8.7 Managing emerging technologies and ethical risk

Multi-agency staff must stay alert to the ethical risks posed by emerging technologies, such as:
- AI and machine learning: Risks around bias, consent and misinformation.
- Facial recognition and biometric data: Heightened privacy implications for children.
- Data profiling and algorithmic decision-making: Need for transparency and challenge.
- Digital surveillance tools: Potential harm to trust and autonomy if used inappropriately.
- New apps or platforms: Rapid evolution requires constant vigilance and risk assessment.
- Internet of Things (IoT) devices: Security vulnerabilities and privacy concerns.

Where new tools are introduced, they must be risk-assessed, approved by senior leadership and accompanied by clear guidance on safe and ethical use.

## 9. Monitoring and policy review

The policy reflects national legislation, statutory guidance and emerging best practice in online safeguarding. It has been approved by the LSCP Board on [20/11/2025] and is effective from [20/11/2025].

The policy will be reviewed annually. Interim reviews may be triggered by:
- Significant legislative or regulatory changes
- Major incidents or emerging safeguarding risks
- Updates to national guidance
- Learning from serious case reviews or local child safeguarding practise reviews

All services are expected to align their own safeguarding and digital use protocols with this policy and ensure that online safety is embedded in their day-to-day practice and training.

# Appendix A – 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.

The template does *not* replace existing risk assessment and analysis tools for responding to child abuse, neglect and exploitation; instead it aims to enhance these assessment tools by enabling enhanced reflection and analysis of the online elements of harm.

**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:<br>☐ Social Care<br>☐ Police<br>☐ Health/CAMHS<br>☐ Education<br>☐ 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 B – Online safety resource directory

National Resources:

- CEOP (Child Exploitation and Online Protection): www.ceop.police.uk
- Internet Watch Foundation: www.iwf.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Childline: www.childline.org.uk / 0800 1111

Educational Resources:

- ThinkUKnow (CEOP Education): www.thinkuknow.co.uk
- Internet Matters: www.internetmatters.org
- NSPCC Online Safety Hub: www.nspcc.org.uk/keeping-children-safe/online-safety
- Parent Zone: www.parentzone.org.uk
- Childnet: www.childnet.com
- Act Early: https://actearly.uk/radicalisation/online-safety/

Professional Resources:

- SWGfL 360 Safe Tool: www.360safe.org.uk
- UK Council for Internet Safety: www.gov.uk/government/organisations/uk-council-for-internet-safety
- Project Evolve: www.projectevolve.co.uk (suggested resource)
- Prevent Guidance: Prevent duty guidance: England and Wales (2023) - GOV.UK
- Report Online Material Promoting Terrorism or Extremism: www.gov.uk/report-terrorism

Lambeth Specific:

- LSCP Website: www.lambethsaferchildren.org.uk
- Lambeth Children's Social Care:
    - 0207 925 3100 (office hours) / 0207 926 555 (out of hours)
    - helpandprotection@lambeth.gov.uk
    - Referral form
- LSCP Multi-Agency Escalation Policy

Key Documents:

- Pan London Threshold Document
- London Safeguarding Children Procedures
- Lambeth Multi-Agency Arrangements to Safeguard Children
- Lambeth Neglect Toolkit (including digital neglect indicators)

Reporting Harmful Content:

- Report Remove (for self-generated images): www.report-remove.com
- Individual platform reporting (check platform safety centres)

Specialist Support:

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- SWGfL Professionals Online Safety Helpline: 0344 381 4772

# Appendix C – Glossary of terms

- **4 Cs:** The UKCIS model categorising online risks - Content, Contact, Conduct, Commerce
- **CEOP:** Child Exploitation and Online Protection Command (part of National Crime Agency)
- **Cyberbullying:** Bullying using electronic communication
- **Deepfake:** Digitally altered video/image created using AI to misrepresent someone
- **Digital Citizenship:** Responsible and positive use of technology
- **Digital Footprint:** Trail of data left by online activities
- **Digital Neglect:** Failure to meet a child's online safety and wellbeing needs
- **DSL:** Designated Safeguarding Lead
- **Grooming:** Building a relationship to manipulate, exploit and abuse
- **LSCP:** Lambeth Safeguarding Children Partnership
- **MASH:** Multi-Agency Safeguarding Hub
- **MARAC:** Multi-Agency Risk Assessment Conference
- **NRM:** National Referral Mechanism (for modern slavery/trafficking)
- **Phishing:** Fraudulent attempt to obtain sensitive information
- **Radicalisation:** The process by which a person comes to support terrorism, or forms of extremism leading to terrorism
- **Sextortion:** Sexual exploitation involving threats or blackmail
- **Sexting:** See "Sharing nudes and semi-nudes"
- **Sharing nudes and semi-nudes:** Self-generated sexual imagery (previously called 'sexting')
- **UKCIS:** UK Council for Internet Safety