



Paramount Safeguarding
Specialist Safeguarding Support

Online Safety Policy

Date: July 2026

Review Date: July 2027

Introduction

'Keeping Children Safe in Education (2026)' requires all Local Authorities and schools to ensure children are safeguarded from harmful and inappropriate online material.

We adhere to all safeguarding and online safety policies and procedures when working within each school/education setting.

We will model safe, responsible behaviour and report any concerns promptly to the setting's Designated Safeguarding Lead.

We adhere to:

- The Local Authority and School online safety expectations and safeguarding policies
- UK GDPR and Data Protection Act 2018
- Online Safety Act 2023
- BACP/UKCP ethical codes for digital practice
- School Acceptable Use Policies and Requirements (if using school systems)

Roles and Responsibilities:

Director/Lead Therapeutic Practitioner: ensures compliance, training and incident management in liaison with the school/education provision

The DSL/Online Safety Lead is Kyri Mingay

Therapeutic Practitioners: follow school policies and procedures and acceptable use agreements where relevant, uphold clinical standards, raise awareness with pupils where appropriate, challenge online harmful behaviour, and report concerns promptly

School DSL: primary contact for safeguarding and online safety concerns

School IT Teams: support secure access, filtering and monitoring, and device safety

Pupils: use technology responsibly, report concerns and know how to seek help, follow school acceptable use policies

Online Risks:

Therapists must understand risks to pupils including:

Content - exposure to illegal, inappropriate or harmful content – including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

Contact – being subjected to harmful online interaction with other users or AI applications, for example peer to peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, financial or other purposes.

Conduct – behaviour that increases the likelihood for harm for example making, sending and receiving explicit images, including those generated with AI

Commerce – risks such as gambling, inappropriate advertising, phishing and financial scams

Cyberbullying or harassment

Privacy breaches

Extremist and terrorist material online – Counter Terrorism and Security Act 2015 require schools to protect learners

Artificial Intelligence (AI):

Generative AI is developing rapidly and is being used more in education. AI use must be safe, ethical and responsible.

Therapeutic Practitioners should raise awareness for pupils regarding AI where appropriate, helping them to understand benefits and risks and encouraging them to talk to a trusted adult if there are any concerns.

We recognise that AI can introduce risks and pupils may be subject to harmful online interaction with other users or generative AI applications that simulate these.

Therapeutic Practitioners must not enter personally identifiable or sensitive data into AI tools.

Where relevant, only school approved AI tools should be used for schoolwork.

Company and sensitive information should not be entered into AI tools unless approved by the Director.

Where AI has been used for documents, reports and communication, this should be made clear.

Therapeutic Practitioners must report any concerns related to AI to the Director and to the school DSL if within the school setting.

Improper use of AI, including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes will result in termination of freelance work with the Therapeutic Practitioner.

Safe Online Therapeutic Practice

There may be circumstances when our services may be delivered online, usually when there are no other options. It is imperative that the safeguarding procedures set out in this policy are adhered to whether working with clients in person or online.

The online platforms used to deliver some services are:

Microsoft TEAMS

The school/education provider should ensure that any child/young person is logged in via their school/education provider email and not their personal email.

Under no circumstances should sessions take place via social media or messaging apps.

The school/education provider should ensure the parent/carer is informed of any sessions being delivered online and written consent obtained.

If a child/young person is logging in from home, consent should be provided by their parent/carer.

Schools should ensure they have the highest filtering and monitoring systems in place when children and young people are using their school systems for online sessions.

Expectations will be made clear at the beginning of any online sessions, including behaviour and conduct. The session will end if the client does not meet the expectations set out and/or displays any inappropriate behaviour.

The practitioner and client should both ensure the background is neutral or blurred when in an online session.

The practitioner and client should both be appropriately dressed when in an online session.

The online session should not be recorded and if this occurs, the sessions should end immediately.

Waiting room features will be used to verify the participant before admitting them into an online session.

A headset will be used when required to ensure privacy and confidentiality of the client.

Clients should inform the school/education provider if there are any concerns regarding the online sessions and the Director should be informed.

Supporting Children and Young People

Therapeutic Practitioners must:

- Promote digital resilience and safe online behaviour
- Encourage pupils to talk to trusted adults about any worries or concerns
- Integrate online safety education into therapeutic work where appropriate

Responding to Online Safety Concerns

Therapeutic Practitioners must follow school safeguarding policies and procedures and report any online safety and/or safeguarding concerns promptly to the school DSL and the Director/DSL.

All concerns must be recorded on our cause for concern form and sent to Director/DSL.

Director/DSL will follow up with school DSL to ensure actions are taken appropriately

All records and notes must be stored on a secure, encrypted system.

Data Protection

We adhere to UK GDPR and Data Protection Act 2018, and to school and Local Authority Data Protection policies and procedures.

Any concerns will be reported to the DSL and Data Protection Officer.

Cyber Security

Cyber incidents and attacks can have a significant impact on services.

These will often be intentional and unauthorised attempts to access, change or damage data and digital technology.

They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption to services
- financial loss
- reputational damage

Only licensed digital technology is used including operating systems, software programmes and cloud services. Systems are encrypted and protected using anti-malware.

Any cyber security concerns will be reported to Report Fraud and where high-risk data breach has occurred, to the ICO.

Advice may also be obtained by the Data Protection Officer (DPO) in the Local Authority.

Monitoring and Review

This policy will be reviewed annually at the start of each academic year or sooner if legislation changes and/or new risks emerge.