



Organisation: Unmask Your Potential Ltd
Policy owner: Helen Kent
Designated Safeguarding Lead: Helen Kent
Deputy Designated Safeguarding Lead: N/A
Online Safety Lead: Helen Kent
Version: 1.0
Date approved: 01/09/2025
Review date: 31/08/2026

2. Online Safety Policy

2.1 Purpose

Unmask Your Potential Ltd recognises that online safety is an essential part of safeguarding. Children and young people may be exposed to harm through digital devices, social media, online gaming, messaging apps, streaming platforms, websites, artificial intelligence tools, online communities and remote learning environments.

This policy sets out how Unmask Your Potential Ltd will manage online safety during face-to-face and remote provision.

2.2 Online Safety Lead

Online Safety Lead: Helen Kent
Telephone: 07944927395
Email: support@unmaskyourpotential.com

The Online Safety Lead is responsible for:

- Promoting safe online practice
- Supporting staff to understand online risks
- Ensuring remote sessions are delivered safely
- Responding to online safety concerns
- Liaising with the DSL where concerns indicate risk of harm
- Reviewing online safety procedures
- Ensuring staff understand the four areas of online risk: content, contact, conduct and commerce

The Online Safety Lead may also be the DSL.

2.3 The four areas of online risk

Unmask Your Potential Ltd recognises the four key areas of online risk identified in Keeping Children Safe in Education.

Content

Young people may be exposed to illegal, inappropriate or harmful content, including pornography, violence, misogyny, racism, extremist material, self-harm or suicide content, eating disorder content, misinformation, hate content or harmful challenges.

Contact

Young people may be subjected to harmful online interaction with other users, including grooming, exploitation, coercion, cyberbullying, harassment, peer pressure, blackmail, sexual communication or contact from unknown adults.

Conduct

Young people's own online behaviour may place them or others at risk. This includes sharing personal information, bullying, sending or requesting nude or semi-nude images, harmful sexual behaviour online, abusive comments, threats, risky livestreaming or unsafe use of social media.

Commerce

Young people may be exposed to risks such as online gambling, scams, phishing, financial exploitation, inappropriate advertising, in-app purchases, fake job offers, fraud, coercion to transfer money or cryptocurrency-related exploitation.

2.4 Remote sessions

Where Unmask Your Potential Ltd delivers online or remote sessions, the following safeguards will apply:

- Sessions will be arranged through agreed organisational channels
- The platform used will be appropriate and secure
- The young person, parent/carer and commissioner will be informed of session arrangements
- Staff will use professional accounts wherever possible
- Staff will not use personal social media to deliver provision
- Meeting links will not be shared publicly
- Waiting rooms, passwords or access controls will be used where available
- Staff will deliver sessions from an appropriate environment
- Young people will be encouraged to join from a safe and appropriate space
- Recording will not take place unless there is a clear purpose, consent and commissioner agreement
- Any safeguarding concern arising during a remote session will be reported to the DSL immediately
- If a young person appears to be at immediate risk during a remote session, staff will contact emergency services and/or the relevant safeguarding service

2.5 Use of devices and internet during provision

Where internet access or device use is part of provision:

- Use must be linked to the agreed learning or support purpose
- Staff must supervise use appropriately
- Young people must not access harmful, illegal or inappropriate content
- Staff must respond immediately if harmful content is accessed or disclosed
- Any online safeguarding incident must be reported to the DSL
- Personal data must not be shared without appropriate reason and consent
- Staff must not store young people's personal data on personal devices unless authorised and secure

2.6 Social media and communication

Staff must not connect with young people through personal social media accounts. Communication with young people must be through agreed professional channels and in line with the commissioning arrangement.

Staff must not:

- Send private messages from personal accounts
- Share personal photos, opinions or private information with young people
- Follow or friend young people online
- Use disappearing message functions for professional communication
- Engage in informal online conversations outside agreed provision

2.7 Online disclosures or incidents

If a young person discloses online harm, such as grooming, cyberbullying, exploitation, image sharing, threats, blackmail, harmful content or online abuse, staff must:

- Listen and take the concern seriously
- Avoid blaming the young person
- Preserve evidence where appropriate, without viewing or sharing illegal material
- Report to the DSL immediately
- Record the concern accurately
- Follow safeguarding procedures

Staff must not ask young people to forward nude or semi-nude images. If illegal images are received accidentally, staff must not share, save, copy or further distribute them and must seek DSL advice immediately.

2.8 Online safety outside provision

Unmask Your Potential Ltd recognises that online harm may happen outside sessions but still affect the young person's wellbeing, attendance, relationships and safety. Staff

will report concerns to the DSL and, where appropriate, liaise with schools, parents/carers, commissioners or safeguarding agencies.

2.9 Training and awareness

Staff will receive online safety awareness appropriate to their role, including the four areas of risk, remote delivery, professional boundaries, harmful online content, online exploitation and reporting routes.

2.10 Review

This policy will be reviewed annually, or sooner if there are changes to legislation, statutory guidance, Suffolk safeguarding procedures or organisational practice.

This policy will be reviewed annually or sooner if:

- Statutory guidance changes
- Suffolk safeguarding procedures change
- There is a safeguarding incident or serious concern
- Provision changes significantly
- Commissioning requirements change

Approved by: Helen Kent

Role: Director

Signature:



Date: 01/09/2025