



Online Safety Policy

Organisation: Supreme Mentoring Services

Policy Owner: Taj Reid

Role: Founder / Lead Designated Safeguarding Lead

Document Version: 1.0

Date Approved: August 2026

Review Date: August 2027

Review Cycle: Annually, or sooner following changes to legislation, statutory guidance, emerging technology, safeguarding practice or a significant online safety incident



1. Policy Statement

Supreme Mentoring Services (SMS) recognises that digital technology and online communication form an important part of the lives of children and young people.

Technology can provide significant opportunities for learning, communication, creativity and social connection. However, children and young people may also encounter harm through social media, messaging platforms, gaming, online communities, artificial intelligence, live streaming and other digital environments.

SMS is committed to safeguarding children and young people from online harm while supporting them to develop the knowledge, confidence and digital resilience needed to engage with technology safely and responsibly.

Online safety is regarded as an integral part of safeguarding and child protection and not as a separate or solely technical issue.



2. Purpose

The purpose of this policy is to:

- establish clear expectations for safe and professional use of digital technology within SMS;
- protect children and young people from online harm;
- protect staff, mentors and other SMS personnel from inappropriate digital contact or unsafe professional practice;
- establish appropriate professional boundaries for online communication;
- ensure online safety concerns and disclosures are recognised, recorded and escalated appropriately;
- support young people to develop safer and more informed online behaviours;
- ensure that SMS works effectively alongside schools, parents/carers and other agencies when online safeguarding concerns arise; and
- ensure that personal information, photographs, recordings and digital records relating to children are handled appropriately.



3. Scope

This policy applies to all individuals working for or on behalf of Supreme Mentoring Services, including employees, mentors, workers, contractors, volunteers and any other individuals engaged to deliver SMS services.

It applies to SMS activity undertaken:

- within schools and education settings;
- within alternative provision;
- in community settings;
- during off-site activities;
- during remote or online mentoring;
- through SMS-owned or authorised digital systems;
- when using devices as part of SMS delivery; and
- whenever an individual's digital conduct may affect their professional relationship with a child or young person.

Where SMS personnel work within a school or partner organisation, they must also comply with that setting's safeguarding, online safety, acceptable-use, mobile-phone, photography and information-security procedures.

Where those procedures impose a higher standard than this policy, the requirements of the host setting should normally be followed unless doing so would conflict with law or SMS safeguarding procedures.



4. Legal and Statutory Framework

This policy has been developed with regard to relevant legislation and guidance, including:

- Children Act 1989;
- Children Act 2004;
- Education Act 2002;
- Keeping Children Safe in Education 2026;
- Working Together to Safeguard Children 2026;
- Online Safety Act 2023;
- Data Protection Act 2018;
- UK General Data Protection Regulation (UK GDPR);
- Data (Use and Access) Act 2025;
- Equality Act 2010;
- Prevent Duty guidance;
- Department for Education filtering and monitoring standards; and
- relevant Information Commissioner's Office guidance concerning children's personal information.

SMS will review this framework as legislation and statutory guidance develops.



5. Understanding Online Harm

SMS recognises the four broad areas of online risk identified within statutory safeguarding guidance:

Content

Children may be exposed to illegal, inappropriate or harmful material, including:

- pornography;
- violent or distressing content;
- misogynistic or discriminatory material;
- racist or extremist content;
- content promoting self-harm, suicide or eating disorders;
- misinformation and disinformation; and
- material promoting harmful behaviours or attitudes.

Contact

Children may experience harmful interaction with other people online, including:

- grooming;
- sexual exploitation;
- criminal exploitation;
- coercion;
- radicalisation;
- inappropriate contact from adults;
- harmful peer-to-peer contact; and
- contact designed to obtain personal or sexual information.



Conduct

A child's own online behaviour may place themselves or others at risk. This can include:

- cyberbullying;
- sharing sexual images;
- harassment;
- abusive messages;
- sharing private information;
- online aggression;
- harmful online challenges; and
- creating, requesting or distributing inappropriate material.

Commerce

Children may encounter risks associated with:

- online gambling;
- scams and fraud;
- inappropriate advertising;
- financial exploitation;
- phishing;
- in-game purchases; and
- other commercial practices that may exploit children.

SMS also recognises that these risks can overlap and that online harm may form part of wider safeguarding concerns occurring offline.



6. Online Safety Within Mentoring

Mentors occupy a position of trust and must model safe and responsible digital behaviour.

Where technology forms part of a mentoring activity, its use must have a legitimate purpose connected to the young person's support, education or agreed intervention.

Mentors should consider:

- the age and developmental needs of the young person;
- SEND and communication needs;
- known safeguarding vulnerabilities;
- the nature of the content being accessed;
- the environment in which technology is being used;
- the host setting's policies;
- whether appropriate supervision is available; and
- whether the activity could expose the young person to unnecessary risk.

Mentors must not deliberately expose children to inappropriate material as part of an intervention.



7. Professional Communication With Children and Young People

SMS personnel must maintain clear professional boundaries in all digital communication.

Personnel must not:

- give children their personal telephone number or personal email address unless expressly authorised through an agreed SMS arrangement;
- add, follow or accept children on personal social media accounts;
- communicate privately with children through personal social media accounts;
- communicate with children through personal messaging applications without an expressly authorised professional arrangement;
- engage in secretive, sexualised, flirtatious or otherwise inappropriate communication;
- delete professional communications in order to prevent organisational oversight; or
- encourage a child to conceal communication from parents/carers, schools or SMS.

Where direct electronic communication with a young person forms an agreed part of an intervention, an SMS-approved communication method should be used and appropriate safeguarding arrangements established.

Communication must remain professional, proportionate and related to the agreed purpose of the intervention.

Any communication that causes concern must be reported to the DSL.



8. Social Media

SMS personnel are expected to maintain professional boundaries when using social media.

Staff and mentors should consider the potential impact of their public online presence upon their professional role.

Personnel must not use personal social media accounts to establish or maintain relationships with children they support through SMS.

Privacy settings should be appropriately managed, but personnel should recognise that no social media content can be assumed to remain completely private.

Personnel must not publish confidential information relating to a young person, family, school, colleague or SMS.

Images, recordings or information obtained through SMS work must not be published on personal social media accounts.



9. Mobile Phones & Personal Devices

Personal devices must be used responsibly and in accordance with the rules of the setting in which SMS is operating.

SMS personnel must not use personal devices to photograph, film or make audio recordings of children unless there is a legitimate, authorised reason and the appropriate permissions and safeguarding arrangements are in place.

Where a school or commissioning organisation prohibits or restricts mobile-phone use, SMS personnel must comply with those requirements.

Personal devices should not be used in a manner that undermines professional boundaries, safeguarding or the confidence of children, families or partner organisations.



10. Photography, Video and Digital Content

Photographs, video or audio recordings involving children must only be created where there is a clear and legitimate purpose.

Before such material is created or published, SMS will consider:

- the purpose for which it is required;
- the appropriate lawful basis for processing personal information;
- any required permissions or consent;
- the wishes and best interests of the child;
- the child's age and understanding;
- contractual requirements of the commissioning organisation;
- safeguarding risks;
- how the material will be stored; and
- where and how it may be published.

Images or recordings must not be taken simply because a child has verbally agreed at the time.

Content must not be published in a manner that unnecessarily identifies a child, reveals sensitive personal information or creates a foreseeable safeguarding risk.



11. Remote and Online Mentoring

Where mentoring is delivered remotely, the same safeguarding and professional standards apply as during face-to-face delivery.

Before online mentoring takes place, SMS should establish appropriate arrangements regarding:

- the platform being used;
- who has agreed to the online intervention;
- how the young person's identity is confirmed;
- parental/carers or commissioning-setting involvement where appropriate;
- privacy and confidentiality;
- appropriate location for the session;
- recording of sessions;
- emergency contact arrangements; and
- procedures where a safeguarding disclosure is made.

Mentors should conduct online sessions from an appropriate professional environment wherever reasonably practicable.

Sessions must not be recorded unless there is a clear purpose, appropriate authorisation and a lawful basis for doing so.

A young person must never be encouraged to participate in secret online contact with an SMS mentor.



12. Online Gaming and Digital Activities

SMS recognises that gaming and other digital activities can, where appropriately planned, provide legitimate tools for engagement and relationship-building with some children and young people.

Where online gaming or another digital platform forms part of an agreed mentoring intervention:

- there must be a clear mentoring or engagement purpose;
- the activity must be authorised as part of the intervention;
- age ratings and suitability must be considered;
- professional accounts should be used where appropriate;
- personal gaming profiles should not normally be shared with young people;
- communication must remain professional;
- interactions must be appropriately supervised or accountable;
- privacy and safeguarding settings must be considered; and
- the activity must not create an ongoing personal relationship between the mentor and young person outside the agreed intervention.

The use of gaming as an engagement tool does not remove or reduce normal safeguarding and professional-boundary requirements.



13. Artificial Intelligence and Emerging Technologies

SMS recognises that generative artificial intelligence and other emerging technologies may create both opportunities and safeguarding risks.

Personnel must exercise professional judgement when using AI-supported tools as part of their work.

Personally identifiable, confidential, safeguarding or sensitive information concerning children must not be entered into public generative-AI systems unless SMS has specifically authorised the system and established that the processing is lawful and appropriately protected.

AI-generated content used with children should be checked for:

- accuracy;
- age appropriateness;
- bias or discrimination;
- harmful or inappropriate material;
- misinformation; and
- safeguarding implications.

AI-generated output must not replace professional safeguarding judgement.



14. Filtering and Monitoring in Schools and Partner Settings

SMS recognises that schools and colleges have responsibilities for appropriate filtering and monitoring of their IT systems.

Where SMS operates within a school or education setting, personnel must comply with the setting's filtering, monitoring and acceptable-use arrangements.

SMS mentors should:

- understand how to report online safety concerns identified during their work;
- not attempt to bypass filtering or security controls;
- appropriately supervise digital activities within mentoring sessions;
- report suspected weaknesses or inappropriate access where identified; and
- cooperate with the school's DSL and relevant staff when concerns arise.

SMS does not assume responsibility for operating or maintaining a commissioning school's technical filtering and monitoring infrastructure unless this has been expressly agreed as part of a contractual arrangement.



15. Safeguarding Disclosures and Online Incidents

An online safety concern may constitute a safeguarding or child protection concern. Examples include:

- online grooming;
- sexual exploitation;
- criminal exploitation;
- cyberbullying;
- coercive or controlling behaviour;
- threats of violence;
- radicalisation;
- sexual image sharing;
- exposure to harmful or illegal material;
- online harassment;
- financial exploitation;
- concerning contact with adults or peers;
- self-harm or suicide-related online activity; or
- information suggesting that a child or another person may be at risk.

Where a mentor becomes aware of such a concern, they must:

1. prioritise the immediate safety of the child;
2. listen and respond appropriately without conducting their own investigation;
3. preserve relevant information where appropriate and lawful;
4. make an accurate safeguarding record;
5. report the concern promptly to the appropriate DSL in accordance with SMS safeguarding procedures; and
6. cooperate with any subsequent safeguarding action.

Where SMS personnel are working within a school, the school's DSL should normally be informed in accordance with the school's safeguarding procedures, alongside SMS's own safeguarding reporting arrangements where applicable.

If there is an immediate risk of significant harm, emergency or statutory safeguarding procedures must be followed without delay.



16. Child-on-Child Online Abuse

SMS recognises that children can abuse other children online.

This may include:

- cyberbullying;
- sexual harassment;
- sharing nude or semi-nude images;
- coercion to create or share sexual material;
- abusive or threatening messages;
- discriminatory abuse;
- impersonation;
- humiliation;
- exclusion from online groups; and
- sharing images or information without permission.

Such behaviour must not be dismissed as "banter", normal adolescent behaviour or an inevitable part of being online.

Concerns will be considered through SMS safeguarding procedures and, where appropriate, referred to the relevant education setting or statutory agency.

17. Nude and Semi-Nude Images

Where SMS personnel become aware that a child has created, shared or received a nude or semi-nude image, the matter must be treated as a safeguarding concern.

Personnel must not:

- request that the child sends them the image;
- intentionally view an image unless there is an exceptional safeguarding reason and this is consistent with applicable guidance;
- copy or distribute the image;
- save the image onto a personal device; or
- conduct their own investigation.

The matter must be referred promptly to the appropriate DSL and managed in accordance with current safeguarding guidance.



18. Online Radicalisation and Extremism

SMS recognises that children may encounter extremist material, extremist narratives or individuals seeking to radicalise them online.

Personnel should remain professionally curious where significant changes in a young person's language, attitudes, online interests or behaviour give rise to safeguarding concerns.

Concerns regarding radicalisation or extremism must be reported through safeguarding procedures and considered in accordance with applicable Prevent arrangements.

19. Data Protection and Children's Information

SMS recognises that children require particular protection in relation to their personal information.

Personal information must be:

- processed lawfully, fairly and transparently;
- collected for legitimate purposes;
- limited to information that is necessary;
- accurate where required;
- retained only for as long as necessary;
- appropriately secured; and
- shared only where there is a lawful and legitimate reason.

Children's best interests will be an important consideration when SMS processes or shares their personal information. Information must not be stored unnecessarily on personal devices, personal cloud-storage accounts or unauthorised digital platforms.

Safeguarding information may be shared without consent where there is a lawful basis and sharing is necessary and proportionate to protect a child or another person.



20. Cyberbullying and Online Harassment

SMS does not tolerate cyberbullying, discriminatory abuse, harassment or intimidation.

Where a young person discloses cyberbullying or online harassment, mentors should:

- listen without judgement;
- establish sufficient information to understand immediate risk;
- avoid promising absolute confidentiality;
- record relevant information;
- report safeguarding concerns appropriately; and
- support the young person in accordance with their mentoring role and agreed safeguarding plan.

Mentors should not personally confront alleged perpetrators or attempt to investigate disputes between children.

21. Supporting Digital Resilience

SMS aims not only to respond to online harm but, where appropriate to the mentoring intervention, to help young people develop safer digital behaviours.

Mentoring may explore:

- recognising unsafe or manipulative online behaviour;
- privacy and personal information;
- healthy social media use;
- cyberbullying;
- digital footprints;
- respectful online relationships;
- gaming and online communities;
- misinformation and critical thinking;
- online exploitation;
- asking for help;
- managing screen use and wellbeing; and
- understanding that online actions can have offline consequences.



These discussions should be age-appropriate, non-judgemental and responsive to the individual young person's circumstances.

22. Responsibilities

Director / Lead DSL

The Director / Lead DSL has overall responsibility for ensuring that:

- this policy is implemented and reviewed;
- personnel understand online safeguarding expectations;
- online safeguarding concerns are responded to appropriately;
- relevant training and guidance are provided;
- serious concerns are referred to appropriate agencies where necessary; and
- lessons from incidents are incorporated into future practice.

SMS Personnel

All SMS personnel are responsible for:

- reading and following this policy;
- maintaining professional digital boundaries;
- remaining alert to online safeguarding concerns;
- reporting concerns promptly;
- protecting confidential information;
- following host-setting procedures; and
- modelling safe and responsible digital behaviour.

Online safety is everyone's safeguarding responsibility.



23. Breaches of This Policy

A breach of this policy by SMS personnel will be taken seriously.

Depending upon the circumstances, a breach may result in:

- additional supervision or training;
- internal investigation;
- disciplinary or contractual action;
- removal from an assignment;
- notification to a commissioning organisation;
- referral under safeguarding procedures;
- referral to the Local Authority Designated Officer (LADO);
- referral to the Disclosure and Barring Service where applicable; and/or
- referral to the police or another statutory authority.

Safeguarding concerns involving an adult working with children will be managed in accordance with the SMS Safeguarding and Child Protection Policy and applicable statutory guidance.

24. Related SMS Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy;
- Code of Conduct and Professional Boundaries Policy;
- Confidentiality Policy;
- Data Protection and Privacy Policy;
- Whistleblowing Policy;
- Complaints Policy;
- Safer Recruitment Policy;
- Equality, Diversity and Inclusion Policy; and
- Lone Working Policy.



25. Monitoring and Review

Supreme Mentoring Services recognises that online risks, platforms and technologies develop rapidly.

This policy will therefore be reviewed at least annually and sooner where:

- legislation or statutory guidance changes;
- new technologies create significant safeguarding considerations;
- SMS introduces new forms of digital delivery;
- learning arises from an online safety incident; or
- organisational practice changes.

Policy Owner: Taj Reid

Role: Founder / Lead DSL

Date Approved: August 2026

Next Review: August 2027