



SB Mentoring

Offering a foundation for future success

Online Safety Policy 2026-27



Approved by:	Louiza Bruce	Advisory Board	Kirsty Burrridge
Last Reviewed on:	04/09/2026	Next Review by:	September 2027

1. Purpose

This policy protects students, staff, volunteers and SB Mentoring from risks associated with technology, including the internet, digital devices, online platforms, social media, remote learning and generative artificial intelligence (AI). It promotes safe, responsible and positive technology use as part of SB Mentoring's whole-organisation safeguarding approach.

Online safety is a running and interrelated theme within safeguarding, curriculum planning, staff training, the work of the Designated Safeguarding Lead (DSL), parental engagement and the management of technology.

2. Scope

This policy applies to:

- all students, staff, volunteers, contractors and visitors using SB Mentoring devices, networks or online services;
- personal devices used on the premises or for learning, mentoring or work-related purposes;
- on-site, off-site and remote-learning activity;
- communications, social media, messaging, cloud services and video-conferencing; and
- AI systems that generate, alter, recommend or simulate text, images, audio, video or interactions.

3. Objectives

SB Mentoring will:

- safeguard students from harmful online content, contact, conduct and commerce risks;
- maintain mechanisms to identify, intervene in and escalate concerns;
- educate students to become informed and responsible digital citizens;
- support staff to use technology safely, lawfully and professionally;
- maintain proportionate filtering, monitoring, cyber-security and access controls;
- consider the additional online risks faced by students with SEND and other vulnerabilities; and
- comply with safeguarding, Prevent, data-protection and information-security obligations.

4. Roles and responsibilities

4.1 Manager / DSL - Louiza Bruce

- has overall responsibility for this policy and online-safety safeguarding arrangements;
- ensures online-safety concerns are recorded, assessed and escalated appropriately;
- ensures staff receive suitable induction and refresher training;
- works with IT support and the filtering and monitoring lead;
- ensures students' views and needs are considered; and
- reports material risks, incidents and review findings to the Advisory Board.

4.2 Advisory Board

- provides strategic challenge and oversight;
- reviews assurance that filtering and monitoring arrangements are effective; and
- ensures online safety is integrated with safeguarding and organisational risk management.

4.3 Staff and volunteers

- model safe and professional technology use;
- supervise students appropriately and follow acceptable-use rules;
- understand filtering and monitoring responsibilities;
- report concerns promptly to the DSL and do not investigate safeguarding matters independently; and
- use only approved systems for organisational information and AI-assisted work.

4.4 Students

- follow the Student IT Acceptable Use Agreement and mobile-device rules;
- use technology respectfully and never create, request or share harmful or sexualised content;
- protect passwords and personal information; and
- report anything that feels unsafe, upsetting, coercive or suspicious to a trusted adult.

4.5 Parents and carers

- support SB Mentoring's online-safety and mobile-device arrangements;
- encourage safe technology use at home; and
- raise concerns promptly and engage with guidance supplied by SB Mentoring.

5. Acceptable use of technology

- All users must follow the relevant Acceptable Use Agreement.
- Organisational devices, networks and accounts must be used primarily for authorised educational or business purposes.
- Users must not bypass security, filtering or monitoring controls or share access credentials.
- Personal devices must not be used to record, photograph or contact students without authority.
- Social media and communications must not breach confidentiality, professional boundaries or bring SB Mentoring or another person into disrepute.
- Only approved software, services and AI tools may be used for SB Mentoring activity.

6. The four areas of online risk

SB Mentoring uses the KCSIE 2026 '4Cs' as the basis of its online-safety approach:

6.1 Content

Exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny or misandry, antisemitism, self-harm, suicide, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation, fake news and conspiracy theories.

6.2 Contact

Harmful interaction with other users or generative AI applications that simulate interaction, including peer pressure, commercial manipulation, adults posing as children or young adults, grooming and sexual, criminal or financial exploitation.

6.3 Conduct

Online behaviour that causes or increases the likelihood of harm, including cyberbullying, harassment, coercion, non-consensual sharing, and making, sending or receiving explicit images, including images altered or generated using AI.

6.4 Commerce

Risks including online gambling, inappropriate advertising, phishing, fraud, financial scams, in-app purchases and other commercial exploitation.

7. Specific safeguarding risks

Staff must remain alert to online risks that overlap with offline harm, including:

- child-on-child abuse, sexual harassment and sexual violence;
- online grooming, child sexual exploitation and child criminal exploitation;
- radicalisation and extremist content;
- cyberbullying, hate speech, racism, misogyny, misandry and discriminatory abuse;
- coercive or controlling behaviour, stalking and financial exploitation;
- self-harm, suicide content, harmful challenges and online hoaxes;
- deepfakes, deep nudes and AI-generated or digitally altered nude or semi-nude imagery;
- sextortion, blackmail and threats to distribute images;
- misinformation, disinformation and manipulative AI interactions; and
- risks to students with SEND or other vulnerabilities, who may face additional barriers to recognising or reporting harm.

8. Generative AI and synthetic media

- Generative AI may be used only in accordance with SB Mentoring's Artificial Intelligence Policy and approved-tool list.
- Identifiable student, safeguarding, health, SEND or other confidential information must not be entered into an unapproved AI system.
- AI outputs must be checked for accuracy, bias, harmful content, privacy and intellectual-property risks.
- AI must not replace safeguarding judgement, professional decision-making or meaningful human oversight.
- Creating, requesting, possessing or sharing sexualised AI imagery of a child or a person who appears to be a child is prohibited and will be treated as a safeguarding concern.
- Filtering and monitoring requirements apply to the use of generative AI on SB Mentoring systems.

9. Nudes, semi-nudes, deepfakes and deep nudes

For safeguarding purposes, images include photographs, videos, livestreams, digitally altered material and content wholly generated by AI. Every incident involving the making or sharing of nude or semi-nude imagery by or concerning a person under 18 requires a safeguarding response, whether described as consensual or non-consensual.

- The concern must be reported immediately to the DSL or deputy.
- Staff must not ask a student to download, resend or unnecessarily display the imagery.
- Staff must not copy, print or share the imagery except where specifically directed by police or another competent authority.
- The DSL will follow current safeguarding guidance, consider the needs of every child involved and determine whether referral to police, children's social care or another agency is required.

- A safeguarding response will not be replaced by a purely disciplinary response.

10. Mobile phones and personal devices

SB Mentoring operates a mobile-phone-free learning environment by default. Students must not access personal mobile phones during sessions, movement between activities or breaks unless a specific exception has been agreed.

- Devices must be switched off or silenced and stored in the designated secure location or otherwise managed as directed by staff.
- Exceptions may be authorised for medical, SEND, safeguarding, travel or agreed educational reasons and will be documented where appropriate.
- Students must not photograph, record or livestream other people or organisational activity without express permission.
- Staff use of personal devices must comply with professional-boundary, confidentiality and data-protection requirements.
- Misuse will be addressed proportionately under the Behaviour Policy and safeguarding procedures.

11. Education and awareness

Students will receive age-, ability- and developmentally appropriate education that helps them:

- recognise the 4Cs and emerging online harms;
- understand privacy, passwords, consent, healthy relationships and respectful communication;
- recognise grooming, coercion, scams, misinformation and manipulative AI interactions;
- understand the prevalence and harm of deepfakes, pornography and misogynistic influencers;
- evaluate online information and AI outputs critically; and
- know how, when and to whom concerns should be reported.

Education will be inclusive and adapted for students with SEND, language needs or other vulnerabilities. Parents and carers will receive relevant guidance, including information about remote learning and filtering and monitoring arrangements.

12. Filtering and monitoring

SB Mentoring will maintain proportionate filtering and monitoring arrangements designed to block harmful and inappropriate content without unreasonably restricting legitimate teaching, learning or safeguarding education.

12.1 Responsibilities

- The Manager is the senior lead responsible for filtering and monitoring.
- The DSL supports safeguarding interpretation, escalation and review.
- IT support manages technical configuration, testing, alerts and remediation.
- All staff must understand the controls in place, supervise use appropriately and know how to report or escalate concerns.

12.2 Review and testing

- Effectiveness will be reviewed at least once every academic year and after any material incident or system change.
- Reviews will check all relevant internet-connected devices and locations, including portable and remotely used devices where controls apply.
- A written record of tests, findings, decisions and remedial actions will be retained.

- The review will consider student age, vulnerability, frequency of access, the Prevent risk assessment and proportionality.
- Over-blocking will be considered so controls do not unreasonably restrict teaching, learning or safeguarding education.

13. Information security and access management

- Personal information will be protected through appropriate technical and organisational measures.
- Accounts will use individual credentials, appropriate permissions and multi-factor authentication where available and proportionate.
- Access rights will be granted according to role, reviewed periodically and removed promptly when no longer required.
- Software and devices will be securely configured, updated and protected against malware and unauthorised access.
- Backups, incident response and recovery arrangements will be maintained proportionately.
- Suspected phishing, account compromise, data loss or cyber-security incidents must be reported immediately.

14. Remote learning and online communication

- Approved platforms and organisational accounts must be used for remote learning and communication.
- Professional boundaries, suitable environments and appropriate supervision must be maintained.
- Parents and carers will be told which platforms students are expected to access and who they may interact with.
- Recordings may be made only where authorised, necessary and supported by appropriate privacy information.
- One-to-one online contact must follow safeguarding and staff-conduct procedures.

15. Responding to incidents

- All online-safety concerns must be reported promptly to the Manager/DSL or deputy.
- Immediate danger or risk of significant harm must be escalated without delay in accordance with the Safeguarding and Child Protection Policy.
- Staff must preserve relevant information but must not investigate, search devices or view harmful imagery beyond what is necessary to report the concern.
- Incidents will be recorded factually, including actions, decisions and rationale.
- The DSL will consider support for the child, risk to others, parental involvement, information sharing and referral to police, children's social care, Prevent/Channel or specialist agencies.
- Suspected data breaches will also be reported through the data-protection incident procedure.

16. Data protection, images and privacy

- Digital information will be processed in accordance with the UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025 and SB Mentoring's Data Protection Policy.
- Only approved secure systems may be used to store or share student information.
- Images and recordings will be created, used and published only where there is an identified lawful basis and appropriate transparency; consent will be obtained where it is the relevant lawful basis.
- Personal data will be limited to what is necessary, retained only as required and shared only with authorised recipients.
- Privacy settings and location-sharing features will be configured to reduce unnecessary exposure.

17. Staff training

All staff and volunteers will receive online-safety and filtering-and-monitoring training at induction, with updates at least annually and whenever required. Training will include the 4Cs, generative AI, deepfakes and nude or semi-nude imagery, cyber-security, information sharing, reporting routes, Prevent risks, professional boundaries and the additional risks faced by vulnerable students.

18. Review, audit and governance

- The online-safety approach and associated risk assessment will be reviewed at least annually.
- Filtering and monitoring effectiveness will be reviewed at least once every academic year and recorded.
- Reviews will consider incidents, student views, staff feedback, emerging technology, local safeguarding risks and updated statutory guidance.
- Material findings and required actions will be reported to the Advisory Board.
- This policy will be updated sooner where an incident, legal change, technology change or revised government guidance requires it.

19. Related policies

- Safeguarding and Child Protection Policy
- Artificial Intelligence Policy
- Student IT Acceptable Use Agreement
- Staff Code of Conduct
- Behaviour and Anti-Bullying Policy
- Data Protection Policy
- Mobile Phone and Personal Device arrangements
- Whistleblowing and Complaints procedures

Appendix A - Principal guidance

- Department for Education: Keeping children safe in education 2026 (effective 1 September 2026) - <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- Department for Education: Meeting digital and technology standards in schools and colleges - <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges>
- Department for Education: Safe use of generative AI in education - <https://www.gov.uk/government/publications/safe-use-of-generative-ai-in-education-module-3>
- Department for Education: Mobile phones in schools - <https://www.gov.uk/government/publications/mobile-phones-in-schools>
- UK Council for Internet Safety: Sharing nudes and semi-nudes guidance - <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>