Simply Sensory
Training and Support
Creating The Building Blocks For Learning

"Live, Laugh, Learn"

SIMPLY SENSORY
ONLINE SAFETY POLICY

September 2026 - 2028

Reviewed: September 2026

Next Review Date: September 2028 (Every 2 years)

1. Policy Statement

Simply Sensory recognises that technology, the internet, mobile devices, social media, gaming, online communication, artificial intelligence and digital services are an important part of modern life and can provide significant educational, social, communication and employment opportunities for children and young people.

However, online activity can also expose children and young people to significant risks, including abuse, exploitation, bullying, harmful sexual behaviour, sexual exploitation, grooming, radicalisation, extremism, self-harm and suicide content, inappropriate or illegal material, misinformation, disinformation, scams, fraud, manipulation and harmful use of artificial intelligence.

Simply Sensory is committed to protecting and promoting the welfare of children and young people both **online and offline**.

Online safety is therefore regarded as a safeguarding responsibility and is embedded throughout Simply Sensory's safeguarding arrangements, curriculum, risk assessment, staff training and day-to-day practice.

This policy applies whether technology is being used:

- in a pupil's home;
- in a Simply Sensory learning environment;
- in alternative provision;
- in the community;
- during educational visits;
- during remote or online learning;
- on Simply Sensory equipment;
- on a pupil's device where this is part of an educational activity;
- on a staff device where Simply Sensory information or communication is involved; or
- outside the normal learning environment where the activity has a connection to a Simply Sensory pupil, staff member or educational activity.

Simply Sensory recognises that safeguarding is everyone's responsibility and that children should receive the right help at the right time.

2. Purpose of the Policy

The purpose of this policy is to:

1. protect children and young people from online harm;
2. provide clear expectations for safe and professional use of technology;
3. ensure staff understand their safeguarding responsibilities in relation to online activity;
4. support children and young people to develop the knowledge and skills required to use technology safely;

5. establish clear procedures for responding to online safeguarding concerns;
6. protect confidential and personal information;
7. establish appropriate expectations for mobile phones, cameras, social media, email and messaging;
8. provide appropriate safeguards around artificial intelligence;
9. ensure appropriate filtering, monitoring and supervision;
10. support children with SEND and communication difficulties to access online safety education in an accessible and individualised way;
11. ensure online safety concerns are recorded, investigated and escalated appropriately;
12. ensure Simply Sensory works effectively with parents/carers, social care, police, health services, local authorities and other safeguarding partners where necessary.

3. Legislative and Statutory Framework

This policy has been developed with regard to current legislation, statutory guidance and recognised safeguarding guidance applicable in England.

The principal framework includes:

Safeguarding

- **Children Act 1989**
- **Children Act 2004**
- **Education Act 2002**
- **Education Act 2011**
- **Keeping Children Safe in Education 2026 (KCSIE)** – statutory guidance, in force from 1 September 2026
- **Working Together to Safeguard Children 2026**
- **Education and Inspections Act 2006**, where applicable
- **Safeguarding Vulnerable Groups Act 2006**
- **Children and Social Work Act 2017**
- **Domestic Abuse Act 2021**
- **Online Safety Act 2023**
- relevant local safeguarding partnership procedures and local authority safeguarding arrangements.

KCSIE 2026 replaced the previous edition from 1 September 2026.

Working Together to Safeguard Children 2026 applies to education providers and organisations working with children in England and replaced the 2023 edition.

Data protection and information security

- **UK General Data Protection Regulation (UK GDPR)**
- **Data Protection Act 2018**
- **Data (Use and Access) Act 2025**

- **Privacy and Electronic Communications Regulations 2003 (PECR)**, where applicable
- relevant Information Commissioner's Office (ICO) guidance.

The Data (Use and Access) Act 2025 amends and builds upon existing UK GDPR and Data Protection Act 2018 requirements; Simply Sensory will keep its data protection arrangements under review as further provisions come into force.

Equality and human rights

- **Equality Act 2010**
- **Human Rights Act 1998**
- **Children and Families Act 2014**, including duties relevant to children and young people with SEND.

Simply Sensory will ensure that online safety arrangements do not unfairly discriminate against children with SEND or communication, sensory, cognitive or accessibility needs.

Criminal and online legislation

Relevant legislation includes:

- **Computer Misuse Act 1990**
- **Protection from Harassment Act 1997**
- **Malicious Communications Act 1988**
- **Communications Act 2003**
- **Sexual Offences Act 2003**
- **Protection of Children Act 1978**
- **Criminal Justice Act 1988**, including relevant provisions concerning indecent images
- **Counter-Terrorism and Security Act 2015**
- **Terrorism Act 2000**
- **Online Safety Act 2023**
- relevant copyright and intellectual property legislation.

This list is not exhaustive. Legislation and statutory guidance will be reviewed when this policy is updated.

4. Relationship with Other Simply Sensory Policies

This policy must be read alongside:

- Safeguarding and Child Protection Policy;
- Child Protection Procedures;
- Staff Code of Conduct;

- Behaviour Policy;
- Anti-Bullying Policy;
- Prevent/Radicalisation procedures;
- Whistleblowing Policy;
- Complaints Policy;
- GDPR/Data Protection Policy;
- Information Sharing guidance within GDPR policy;
- Health and Safety Policy;
- Allegations Against Staff within Whistleblowing policy and complaints policy
- Safer Recruitment Policy;
- Risk Assessment Policy;
- Lone Working Policy;
- Remote Learning procedures;
- Sexual Harassment and Sexual Violence procedures.

Where there is a conflict between this policy and the Safeguarding and Child Protection Policy, safeguarding procedures take priority.

5. Scope

This policy applies to:

- all employees;
- tutors;
- teachers;
- support workers;
- managers;
- volunteers;
- agency staff;
- contractors;
- visitors where relevant;
- pupils;
- parents/carers where relevant to their use of Simply Sensory systems.

It applies to technology including:

- computers;
- laptops;
- tablets;
- mobile phones;
- smart phones;
- smart watches;
- cameras;
- webcams;
- gaming devices;
- social media;
- email;

- messaging applications;
- video conferencing;
- online learning platforms;
- cloud storage;
- websites;
- streaming services;
- artificial intelligence tools;
- generative AI;
- educational apps;
- virtual reality;
- connected sensory technology;
- removable storage devices.

6. Online Safety and Safeguarding

Simply Sensory recognises four broad areas of online risk:

Content

Children may encounter harmful, inappropriate, illegal or age-inappropriate material.

This can include:

- pornography;
- violent or graphic content;
- hate material;
- extremist material;
- self-harm and suicide content;
- eating-disorder content;
- gambling;
- substance-related content;
- discriminatory content;
- misinformation;
- disinformation;
- conspiracy theories;
- harmful AI-generated content.

Contact

Children may be contacted by people who intend to:

- groom;
- exploit;
- manipulate;
- abuse;
- sexually exploit;
- financially exploit;

- radicalise;
- bully;
- threaten or coerce them.

Conduct

Children may participate in or be affected by:

- cyberbullying;
- harmful sexual behaviour;
- sexual harassment;
- sharing intimate images;
- impersonation;
- hacking;
- online abuse;
- harassment;
- stalking;
- exclusion;
- discriminatory behaviour.

Commerce

Children may be exposed to:

- scams;
- fraud;
- phishing;
- financial exploitation;
- gambling;
- inappropriate purchases;
- identity theft;
- pressure to provide money or personal information.

Online safety education will reflect these risks and the individual needs and vulnerabilities of each pupil.

7. Online Safety Education

Simply Sensory will provide age- and developmentally appropriate online safety education.

Online safety will be embedded into learning and safeguarding rather than treated as a one-off lesson.

Teaching may include:

- keeping personal information private;
- safe passwords;

- recognising unsafe websites;
- understanding online friendships;
- recognising grooming;
- cyberbullying;
- online reputation;
- consent and respectful communication;
- harmful sexual behaviour;
- sharing nudes and semi-nudes;
- self-harm and suicide content;
- radicalisation and extremism;
- misinformation and disinformation;
- scams and fraud;
- artificial intelligence;
- digital footprints;
- social media;
- gaming;
- reporting concerns;
- blocking and reporting users;
- knowing when to seek help.

Teaching will be adapted for pupils with SEND, including those who use:

- visual communication;
- symbols;
- objects of reference;
- AAC;
- simplified language;
- social stories;
- repetition;
- modelling;
- sensory approaches.

Children will be taught that they should tell a trusted adult if something online makes them frightened, uncomfortable, confused or unsafe.

8. Safeguarding Concerns Arising Online

Any online concern which may indicate that a child is at risk of harm must be treated as a safeguarding concern.

Staff must:

1. listen calmly;
2. reassure the child;
3. avoid making promises of confidentiality;
4. avoid investigating unnecessarily;
5. record the concern accurately;

6. report the concern to the DSL without delay;
7. follow the Safeguarding and Child Protection Policy.

If you are concerned about someone making inappropriate or sexual contact with a child online report to ceop.police.uk

If a child is in immediate danger, staff should contact the emergency services on **999** and inform the DSL/management as soon as practicable.

KCSIE 2026 requires staff to act immediately on safeguarding concerns and report concerns to the DSL or deputy without delay.

9. Online Grooming and Exploitation

Staff must remain alert to online grooming and exploitation.

Potential indicators include:

- secrecy around devices;
- sudden new online friendships;
- receiving unexplained gifts or money;
- significant changes in behaviour;
- withdrawing from family or trusted adults;
- increased anxiety;
- sexualised behaviour or language;
- receiving inappropriate messages;
- unexplained photographs;
- threats or blackmail;
- being encouraged to move conversations to private platforms;
- contact with significantly older individuals;
- being encouraged to meet someone known only online.

If you are concerned about someone making inappropriate or sexual contact with a child online report to ceop.police.uk

If a child is in immediate danger, staff should contact the emergency services on **999** and inform the DSL/management as soon as practicable.

KCSIE 2026 requires staff to act immediately on safeguarding concerns and report concerns to the DSL or deputy without delay.

Any concern must be reported immediately to the DSL.

Where appropriate, Simply Sensory will make referrals to children's social care, police or other safeguarding agencies.

10. Cyberbullying and Online Harassment

Cyberbullying will be treated as a safeguarding and behavioural concern.

This includes:

- abusive messages;
- threats;
- humiliating images;
- exclusion from online groups;
- impersonation;
- spreading rumours;
- discriminatory abuse;
- harassment;
- threatening posts;
- sharing private information;
- creation of fake accounts.

Where cyberbullying may constitute abuse, a criminal offence or a safeguarding concern, the DSL will consider referral to appropriate external agencies.

11. Sharing Nudes and Semi-Nudes

Simply Sensory will follow the current UK Council for Internet Safety guidance, **Sharing nudes and semi-nudes: advice for education settings working with children and young people**, alongside KCSIE and safeguarding procedures.

Any incident involving the sharing of nudes or semi-nudes by a person under 18 must be reported immediately to the DSL.

Staff must:

- remain calm;
- reassure the child;
- avoid blaming or shaming;
- not ask the child to send or show the image;
- not copy, save, print, forward or distribute the image;
- not intentionally view an image unless there is a clear and necessary safeguarding reason consistent with current guidance;
- preserve relevant information without reproducing the image;
- refer the matter to the DSL immediately.

If an adult is involved in creating, requesting, possessing or distributing an indecent image of a child, this must be treated as a serious safeguarding concern and referred immediately to the DSL and, where appropriate, police and children's social care.

Current guidance states that staff should not intentionally view nudes/semi-nudes and must never copy, print, share, store or save such imagery.

12. Searching and Confiscating Devices

Simply Sensory is an alternative education provider and staff must not assume that statutory school powers to search pupils automatically apply to Simply Sensory staff.

Where a device is believed to contain material relevant to a safeguarding concern:

- staff should not conduct an informal investigation;
- staff should not browse through the device unnecessarily;
- the device should be secured where appropriate;
- the DSL/management should be informed;
- police or children's social care should be contacted where appropriate;
- any action must be proportionate and consistent with the child's welfare and legal rights.

Where Simply Sensory is operating within a school, PRU, local authority or other education provider's premises, staff must follow that organisation's authorised searching and confiscation procedures.

DfE searching guidance specifically covers schools, including pupil referral units, but does not automatically confer those statutory powers on every alternative education provider.

13. Filtering and Monitoring

Simply Sensory will take appropriate and proportionate steps to protect children from harmful online material.

Filtering is designed to prevent access to illegal, inappropriate and potentially harmful content.

Monitoring is designed to identify concerning activity and enable an appropriate safeguarding response.

Where Simply Sensory provides or manages internet-connected devices, it will ensure that:

- appropriate filtering is used where technically available;
- monitoring arrangements reflect the risks associated with the pupil and setting;
- staff supervise children appropriately;
- concerns identified through monitoring are reported;

- high-risk safeguarding alerts are acted upon promptly;
- filtering and monitoring arrangements are reviewed regularly;
- staff know how to report inappropriate content;
- filtering and monitoring do not replace active supervision.

DfE guidance states that filtering and monitoring should be reviewed at least annually and should take account of the particular needs and risks of the setting, including use of devices away from the main education environment.

Because Simply Sensory works in pupils' homes and the community, staff must recognise that technical filtering may not be available on every network or personal device. In these circumstances, **active supervision, risk assessment, education and professional judgement** remain essential.

14. Home and Community-Based Learning

Because Simply Sensory frequently delivers education in pupils' homes and community settings, staff must consider online safety as part of the individual risk assessment.

Staff should consider:

- who else may have access to devices;
- whether the home network is filtered;
- whether siblings or other people are present;
- whether the pupil has unrestricted internet access;
- whether the pupil uses social media;
- whether the pupil has access to gaming platforms;
- whether the pupil communicates with unknown individuals;
- whether staff are using a Simply Sensory or personal device;
- whether sensitive information could be seen by others;
- whether photographs or recordings could be taken.

Staff must never assume that a home environment provides the same digital safeguards as an educational establishment.

15. Staff Use of Mobile Phones

Staff must maintain professional boundaries at all times.

Staff:

- must use the Simply Sensory work phone for work-related communication where provided;
- must not give pupils their personal mobile number;

- must not communicate with pupils through personal social media accounts;
- must not communicate with pupils through personal messaging accounts;
- must not use personal devices to store Simply Sensory confidential information;
- must not photograph pupils using personal devices;
- must not record pupils on personal devices;
- must not use personal cloud storage for Simply Sensory information.

Any exception must be specifically authorised by Simply Sensory management and appropriately risk assessed.

16. Communication with Parents and Carers

Communication with parents/carers must take place through approved Simply Sensory communication systems.

Staff must not:

- use personal email addresses;
- use personal social media accounts;
- use personal messaging accounts;
- establish inappropriate private relationships with parents/carers;
- share personal information unnecessarily.

Where an agreed work communication system such as WhatsApp is used, staff must follow Simply Sensory's communication and data protection procedures and must ensure professional boundaries are maintained.

17. Email

Staff must use their Simply Sensory work email for professional communication.

Staff must:

- check recipients carefully;
- check attachments before sending;
- avoid unnecessary personal information;
- use appropriate professional language;
- consider whether information is confidential;
- use secure methods for sensitive information;
- report suspicious or phishing emails;
- report accidental disclosure immediately.

Emails should not be regarded as private simply because they are sent electronically.

Simply Sensory may retain or monitor work communications where lawful, necessary and proportionate.

18. Social Media

Staff must maintain professional boundaries online.

Staff must not:

- follow or add pupils to personal social media accounts;
- communicate privately with pupils through social media;
- post confidential information about pupils;
- post photographs of pupils without appropriate authorisation;
- discuss safeguarding cases online;
- identify pupils or families in personal social media posts;
- publish information that could bring Simply Sensory or their professional role into disrepute.

Staff should remember that online content may remain accessible even after deletion.

19. Photography and Video

Photographs and recordings of children may only be taken for legitimate educational, safeguarding or organisational purposes.

Appropriate consent and/or another lawful basis must be established before photographs are taken or used, in accordance with Simply Sensory's data protection arrangements.

Images must:

- be taken using an approved device;
- be stored securely;
- only be used for the stated purpose;
- not be transferred to personal devices;
- not be posted on personal social media;
- not be shared with unauthorised persons.

Simply Sensory will maintain appropriate records of consent and will respect any withdrawal of consent.

20. Data Protection and Confidentiality

Simply Sensory recognises that safeguarding information is highly sensitive.

All staff must comply with:

- UK GDPR;
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Simply Sensory's Data Protection Policy;
- Information Sharing Policy.

Personal data must only be:

- collected where necessary;
- accessed by authorised individuals;
- used for legitimate purposes;
- stored securely;
- shared lawfully and proportionately;
- retained in accordance with Simply Sensory's retention arrangements.

Data protection must **not** be used as a reason to prevent necessary safeguarding information being shared.

Current statutory information-sharing guidance confirms that information sharing is an important part of safeguarding and that data protection is not a barrier where information needs to be shared to protect a child.

21. Password Security

Staff must:

- use strong passwords;
- keep passwords confidential;
- not share passwords;
- not write passwords where they can be accessed by others;
- use multi-factor authentication where available;
- report suspected compromise immediately;
- lock devices when unattended.

Passwords must not be shared with pupils.

22. Cyber Security

Staff must remain alert to:

- phishing;
- malware;
- ransomware;
- suspicious links;

- suspicious attachments;
- fraudulent emails;
- identity theft;
- unauthorised access;
- data breaches.

If a staff member believes a Simply Sensory device or account has been compromised, they must:

1. stop using the device/account where appropriate;
2. avoid deleting evidence;
3. report the concern immediately to management;
4. follow Simply Sensory's data breach procedure.

23. Artificial Intelligence

Simply Sensory recognises the increasing use of generative AI.

AI may provide educational benefits but can create safeguarding, privacy, misinformation, bias, manipulation and data protection risks.

Staff must not enter confidential pupil information, safeguarding information, medical information or other sensitive personal data into an AI system unless the system has been specifically approved by Simply Sensory and appropriate data protection safeguards are in place.

AI must not replace professional judgement.

Staff must consider:

- accuracy;
- bias;
- misinformation;
- inappropriate content;
- safeguarding risks;
- privacy;
- copyright;
- data protection;
- age appropriateness;
- SEND accessibility;
- emotional and psychological impact.

Where children use generative AI, this must be age-appropriate, supervised where necessary and consistent with the pupil's individual risk assessment.

DfE's 2026 generative AI product safety standards specifically address filtering, monitoring, privacy, security, cognitive development, emotional and social development, mental health and manipulation.

24. Misinformation, Disinformation and Conspiracy Theories

Children will be supported to develop critical thinking skills.

Staff should help pupils understand that online information may be:

- inaccurate;
- deliberately misleading;
- manipulated;
- generated by AI;
- taken out of context;
- designed to influence or exploit them.

Where online content appears to promote extremism, terrorism, hatred or other safeguarding risks, this must be reported to the DSL.

25. Radicalisation and Extremism

Online activity may be a pathway through which children encounter extremist material or individuals seeking to radicalise them.

Staff must remain alert to:

- extremist content;
- increasingly rigid or hateful views;
- promotion of violence;
- attempts to recruit others;
- extremist online communities;
- contact with individuals promoting extremist ideology.

Concerns must be reported through Simply Sensory safeguarding procedures.

The DSL will consider whether Prevent or other appropriate referral pathways are required.

26. Self-Harm and Suicide Content

Online content relating to self-harm or suicide can increase risk for vulnerable children.

Staff must report concerns where a child:

- searches for methods of self-harm or suicide;
- shares concerning material;
- joins online self-harm communities;

- receives encouragement to self-harm;
- appears to be influenced by online content;
- communicates suicidal thoughts online.

Such concerns must be managed through safeguarding and the child's individual risk assessment.

Immediate risk requires urgent action.

27. Online Sexual Harassment and Harmful Sexual Behaviour

Simply Sensory recognises that sexual harassment and harmful sexual behaviour can occur online as well as face-to-face.

This includes:

- sexualised messages;
- unwanted sexual images;
- sexual threats;
- sexual comments;
- sharing sexualised images;
- coercion;
- sexualised bullying;
- online grooming;
- pressure to send images;
- sexual extortion.

If you are concerned about someone making inappropriate or sexual contact with a child online report to ceop.police.uk

If a child is in immediate danger, staff should contact the emergency services on **999** and inform the DSL/management as soon as practicable.

KCSIE 2026 requires staff to act immediately on safeguarding concerns and report concerns to the DSL or deputy without delay.

All concerns must be reported to the DSL.

The welfare and safety of all children involved must be considered.

28. Online Reputation and Digital Footprint

Children will be supported to understand that online activity can have long-term consequences.

They will be encouraged to consider:

- what they post;
- who can see it;
- whether it could identify them;
- whether it could harm them or another person;
- whether it could affect education or employment;
- whether an image can be removed once shared.

29. Gaming

Gaming can provide valuable social and educational opportunities but may also create safeguarding risks.

Staff should be aware of:

- online strangers;
- inappropriate chat;
- grooming;
- bullying;
- financial exploitation;
- gambling-like features;
- inappropriate content;
- excessive use;
- exposure to extremist or harmful material.

Concerns must be reported through safeguarding procedures.

30. Remote and Online Learning

Where remote learning is used:

- staff must use approved platforms;
- professional boundaries must be maintained;
- lessons must be appropriately supervised;
- safeguarding procedures continue to apply;
- personal information must be protected;
- recording must only occur where authorised;
- children must not be required to reveal unnecessary information about their home environment;
- staff must report safeguarding concerns immediately.

DfE guidance confirms that normal safeguarding and staff behaviour expectations continue to apply during remote education.

31. Online Safety for Children with SEND

Simply Sensory recognises that children with SEND may experience additional online vulnerabilities.

Some children may:

- find it difficult to recognise manipulation;
- have difficulty understanding social relationships;
- interpret online communication literally;
- struggle to identify unsafe behaviour;
- be more susceptible to grooming;
- have limited understanding of permanence;
- communicate differently;
- require additional support to report concerns.

Online safety education will therefore be adapted to each child's:

- developmental level;
- communication style;
- cognitive ability;
- sensory profile;
- individual risk;
- EHC plan where applicable.

32. Reporting an Online Safety Incident

Any member of staff who becomes aware of an online safety concern must report it to the DSL without delay.

The concern should be recorded factually, including:

- what was disclosed or observed;
- date and time;
- who was involved;
- actions taken;
- who was informed;
- decisions made;
- rationale for decisions;
- referrals made;
- outcomes.

KCSIE 2026 specifically emphasises that safeguarding records should include the concern, actions, decisions, rationale and outcomes.

33. Information Sharing

Simply Sensory will share information where necessary to safeguard a child.

Information will be:

- relevant;
- proportionate;
- accurate;
- timely;
- securely communicated;
- shared only with appropriate people/agencies.

Consent will not be treated as an absolute requirement where information must lawfully be shared to safeguard a child.

The current statutory information-sharing guidance was updated in September 2026 and confirms the importance of lawful information sharing in safeguarding.

34. Multi-Agency Working

Where an online safety concern indicates possible abuse, exploitation or significant harm, Simply Sensory will work with relevant agencies, which may include:

- children's social care;
- police;
- local safeguarding partners;
- health professionals;
- CAMHS or other mental health services;
- Prevent;
- the local authority;
- education providers;
- parents/carers, where appropriate and safe.

Simply Sensory will follow local safeguarding procedures and referral pathways.

35. Allegations or Concerns About Staff

Any online safety concern involving a member of staff must be treated seriously.

This includes allegations that a member of staff has:

- communicated inappropriately with a pupil;
- contacted a pupil through a personal account;
- shared inappropriate material;
- photographed a pupil without authorisation;
- sent inappropriate messages;
- accessed inappropriate material;
- breached confidentiality;
- engaged in online grooming or sexualised communication.

The concern must be reported immediately through Simply Sensory's safeguarding and allegations procedures.

Where required, the Local Authority Designated Officer (LADO), police or other agencies will be contacted.

Staff must not investigate allegations against colleagues themselves.

36. Whistleblowing

Staff have a responsibility to raise concerns where they believe safeguarding arrangements are inadequate.

Concerns should normally be raised with:

- the DSL;
- Deputy DSL;
- Simply Sensory management.

If a staff member feels unable to raise the concern internally, they should use the whistleblowing arrangements available to them, including appropriate external safeguarding or professional channels.

KCSIE 2026 confirms the importance of effective whistleblowing arrangements as part of safeguarding.

37. Monitoring and Review

Simply Sensory Management will monitor the effectiveness of this policy.

This will include consideration of:

- online safety incidents;
- safeguarding referrals;
- staff training;
- filtering;
- monitoring;

- device security;
- data breaches;
- pupil feedback;
- parent/carer concerns;
- changes in technology;
- emerging online harms;
- changes in legislation and statutory guidance.

Filtering and monitoring arrangements will be reviewed at least annually and sooner where there is a significant change in risk, technology or safeguarding arrangements.

38. Staff Training

All staff will receive appropriate safeguarding and online safety training.

Training will include:

- KCSIE requirements;
- online safeguarding;
- online grooming;
- cyberbullying;
- harmful sexual behaviour;
- sharing nudes and semi-nudes;
- radicalisation;
- self-harm and suicide content;
- misinformation and disinformation;
- AI;
- data protection;
- confidentiality;
- professional boundaries;
- social media;
- reporting procedures.

Training will be updated where legislation, statutory guidance or significant online risks change.

39. Responsibilities

Simply Sensory Management

Management is responsible for:

- ensuring this policy is implemented;
- ensuring appropriate safeguarding arrangements are in place;
- ensuring staff receive training;

- ensuring appropriate technology is available;
- reviewing filtering and monitoring;
- ensuring incidents are recorded;
- ensuring serious incidents are escalated;
- ensuring policies remain current.

Designated Safeguarding Lead

The DSL is responsible for:

- responding to online safeguarding concerns;
- maintaining safeguarding records;
- advising staff;
- making referrals;
- liaising with external agencies;
- ensuring online safety forms part of safeguarding training;
- reviewing online safety risks;
- contributing to filtering and monitoring reviews.

All Staff

All staff are responsible for:

- maintaining professional boundaries;
- following this policy;
- completing required training;
- protecting personal information;
- supervising pupils appropriately;
- reporting concerns immediately;
- recording concerns accurately;
- never assuming that someone else will report a concern.

40. Staff Acceptable Use Agreement

All Simply Sensory staff must agree to the following:

I will:

1. use Simply Sensory technology responsibly;
2. use approved systems for Simply Sensory business;
3. keep passwords secure;
4. protect confidential information;
5. comply with UK GDPR and the Data Protection Act 2018;
6. comply with Simply Sensory data protection procedures;
7. use work communication systems appropriately;
8. maintain professional boundaries online;

9. never communicate with pupils through personal social media accounts;
10. never give pupils my personal contact details unless specifically authorised;
11. never photograph pupils using a personal device;
12. never store pupil information on a personal device or personal cloud account;
13. report safeguarding concerns immediately;
14. report suspected data breaches immediately;
15. follow procedures relating to nudes and semi-nudes;
16. use AI responsibly and never enter confidential pupil information into unauthorised AI systems;
17. respect copyright and intellectual property;
18. not access, download, store or distribute illegal or inappropriate material;
19. not post confidential or inappropriate information about Simply Sensory, pupils or colleagues online;
20. ensure my online behaviour does not bring my professional role or Simply Sensory into disrepute.

I understand that Simply Sensory may monitor the use of Simply Sensory systems where this is lawful, necessary and proportionate.

41. Pupil Acceptable Use

Pupils will be supported to:

- use technology safely;
- respect others online;
- keep passwords private;
- protect personal information;
- report bullying;
- report inappropriate content;
- tell an adult if someone online makes them uncomfortable;
- not share intimate images;
- not share other people's images without permission;
- use technology appropriately;
- understand that online behaviour can have real-world consequences.

Rules will be adapted to the pupil's age, developmental stage, communication needs and understanding.

42. Parents and Carers

Parents and carers are encouraged to:

- talk to their child about online safety;
- understand the platforms their child uses;
- establish appropriate boundaries;

- encourage children to report concerns;
- monitor online activity where appropriate;
- report serious safeguarding concerns to Simply Sensory.

Simply Sensory will provide advice and support where appropriate.

43. Breaches of this Policy

A breach of this policy may result in:

- safeguarding action;
- additional training;
- management investigation;
- disciplinary action;
- referral to external agencies;
- referral to the police where a criminal offence may have occurred.

Any response will be proportionate and will consider the circumstances and welfare of those involved.

44. Review

This policy will be formally reviewed at least annually and sooner where required.

The next scheduled review is:

September 2027

The policy will also be reviewed following:

- significant changes to KCSIE;
- changes to Working Together to Safeguard Children;
- changes to data protection legislation;
- significant technological developments;
- serious online safety incidents;
- changes to local safeguarding arrangements;
- changes to Simply Sensory's provision.

45. Key Guidance and Reference Documents

Staff should be familiar with the following current guidance, as relevant to their role:

- **Keeping Children Safe in Education 2026**
- **Working Together to Safeguard Children 2026**
- **Information Sharing: Advice for Practitioners Providing Safeguarding Services**
- **Sharing nudes and semi-nudes: advice for education settings working with children and young people**
- **Searching, Screening and Confiscation**
- **Meeting Digital and Technology Standards in Schools and Colleges – Filtering and Monitoring**
- **Generative AI: Product Safety Standards**
- relevant DfE data protection guidance
- relevant ICO guidance
- local safeguarding partnership procedures
- local authority safeguarding procedures.

Appendix 1 – Immediate Online Safety Response

If a child tells you something has happened online:

DO

- remain calm;
- listen;
- reassure;
- take the concern seriously;
- explain that you need to share the information with the appropriate safeguarding person;
- record accurately;
- report to the DSL immediately.

DO NOT

- promise secrecy;
- blame the child;
- investigate unnecessarily;
- ask leading questions;
- ask the child to forward inappropriate images;
- copy or save illegal images;
- send images to yourself or another person;
- post about the incident online;
- attempt to resolve a serious safeguarding matter yourself.

If the child is in immediate danger:

Call 999 and then inform the DSL/management as soon as possible.

Appendix 2 – Online Safety Incident Record

Child's name: _____

Date: _____

Time: _____

Member of staff receiving concern: _____

Nature of concern:

_____

_____

What was disclosed/observed:

_____

_____

Immediate action taken:

_____

DSL informed: Yes / No

Time DSL informed: _____

Further action/referral:

_____

Reason for decisions made:

_____

Outcome:

_____

Staff signature: _____

DSL signature: _____

Date: _____

Appendix 3 – Policy Statement

Simply Sensory recognises that:

Safeguarding is everyone's responsibility.

Children and young people have the right to learn, communicate, explore and participate online in an environment where their safety, dignity and wellbeing are protected.

Simply Sensory will therefore seek to provide children and young people with the skills, support and confidence to use technology safely while responding promptly and appropriately to any indication that a child may be at risk of harm.