Version:	**1.0**
Relevant to:	**All Staff & Stakeholders**
Document Issue Date:	**24/09/2025**
Implementation Date:	**24/09/2025**
Next review Date:	**23/09/2026**
Author:	**Kim Webster-Marsh (CEO)**

Signed - 

Online Safety Policy

Building SEND Castles Ltd

1. Policy Statement

Building SEND Castles Ltd is committed to ensuring the safety and wellbeing of children, staff, and volunteers when using digital technologies. This policy outlines our approach to online safety, recognising that digital technologies play an increasing role in learning, communication, and administration.

Building SEND Castles Ltd is registered with the ICO

This policy complements our Safeguarding Policy, Whistleblowing Policy, and Data Protection practices.

2. Scope

This policy applies to:

- All staff, volunteers, and trustees
- All children and young people attending our provision
- Contractors or visitors accessing our digital systems

It covers the use of:

- The internet
- Email and messaging services
- Social media
- Learning platforms
- Tablets, smartphones, laptops, and any other digital device used on site or during remote sessions

3. Online Safety Lead

Online Safety Lead (OSL): Kim Webster-Marsh (CEO/DSL/DPO)
Contact: buildingsendcastles@gmail.com / 07879793763

Role and Responsibilities:

- Oversee implementation of the Online Safety Policy
- Ensure staff, volunteers, and children are trained in online safety
- Monitor online safety risks and respond to incidents
- Liaise with external agencies (e.g., Suffolk Safeguarding Partnership, LADO, Police) where required
- Provide regular updates to the Board of Directors
- Ensure compliance with data protection legislation (GDPR, UK Data Protection Act 2018) when handling digital data and online activity

4. Principles of Online Safety

- **Education and Awareness:** All staff will receive online safety training as part of their induction and annual safeguarding refresher.
- **Supervision and Monitoring:** Children will be supervised during all use of technology. Any online activity will be pre-screened and age-appropriate.
- **Appropriate Use:** Children will only use devices and platforms approved by the organisation, and with direct adult supervision.
- **Remote Learning:** Any remote sessions will be delivered via approved platforms, with parental/carer consent and oversight. Children will not be left unsupervised in virtual sessions.

5. Areas of Online Risk (KCSIE 2025)

Staff will monitor and mitigate the following areas of risk:

- **Content:** Exposure to illegal, inappropriate, or harmful material (e.g., pornography, extremist or radicalising material, violent content, misinformation, disinformation, AI-generated harmful content, deepfake material).
- **Contact:** Harmful interaction with other users (e.g., cyberbullying, grooming, exploitation, or online harassment).
- **Conduct:** Children's own online behaviour that may cause harm or put them at risk (e.g., oversharing, sexting, risky challenges, harmful trends, misuse of emerging technologies such as AI tools, VR/AR, or livestreaming).
- **Commerce:** Risks such as online gambling, scams, phishing, or inappropriate advertising.
- **Misinformation/Disinformation:** Being exposed to false, misleading, or manipulated online content that could cause harm.

6. Safeguarding Children with SEND and SLCN

- **Accessibility:** Staff adapt teaching on online safety using visual aids, symbols, and accessible language.
- **Observing Non-Verbal Signs:** Staff are alert to non-verbal indicators of distress or confusion when using technology.
- **Support Tools:** Filters, parental controls, and communication software are used to ensure a safe digital environment.

7. Device Management and Security

- All devices are at least 10 digit password-protected and maintained by authorised staff.
- Personal devices are not permitted for children.
- Children will never be left alone with internet-enabled devices.
- Staff are not permitted to use personal devices for any interaction with children.
- **Filtering & Monitoring:** The organisation ensures appropriate filtering and monitoring systems are in place, reviewed annually, and adjusted to reflect changes in technology and risk.

8. Social Media and Communication

- Staff must never share personal contact details or communicate with children via personal social media accounts or messaging platforms.
- The organisation may use a professional social media page for updates
- Consent from parents/carers will be obtained before sharing any photos or digital content externally.

9. Responding to Online Safety Incidents

- All online safety incidents must be recorded using the safeguarding concern form.
- The Online Safety Lead (DSL) will assess and escalate incidents if necessary (e.g., to the LADO or police).
- Parents/carers will be informed of incidents involving their child where appropriate.

10. Staff Training

- All staff receive online safety training as part of their induction and annual safeguarding refresher.
- Training covers: recognising signs of online harm, risks specific to children with SEND, misinformation/disinformation, AI and emerging technologies, and responding to digital safeguarding concerns.

11. Monitoring and Review

- The Online Safety Policy will be reviewed annually, or earlier in response to incidents, technology changes, or statutory updates.

- Online safety is a standing item in safeguarding audits and team meetings.

12. Contact for Online Safety Concerns

Online Safety Lead (OSL / DSL / DPO): Kim Webster-Marsh
Email: buildingsendcastles@gmail.com
Phone: 07879793763

Appendices

Appendix A – Key Online Safety Contacts

Role	Name	Contact Details
Online Safety Lead (OSL) / DSL / DPO	Kim Webster-Marsh	buildingsendcastles@gmail.com / 07879793763
Deputy DSL (if applicable)	[Insert Name]	[Insert Email / Phone]
Suffolk Safeguarding Partnership	—	www.suffolksp.org.uk / 03456 061 499
Local Authority Designated Officer (LADO)	—	lado@suffolk.gov.uk / 0300 123 2044
Emergency Services (Police)	—	999 (emergency) / 101 (non-emergency)

Appendix B – Online Safety Risk Categories (KCSIE 2025)

Staff must be aware of the key areas of risk outlined in Keeping Children Safe in Education (2025):

- **Content** – Exposure to harmful material, misinformation, disinformation, deepfakes, or AI-generated content.
- **Contact** – Harmful interaction with others online.
- **Conduct** – Risky or harmful behaviour online, including misuse of AI, VR/AR, and livestreaming.
- **Commerce** – Financial or commercial exploitation, scams, and advertising.
- **Misinformation/Disinformation** – Harm from exposure to false or misleading online information.

Appendix C – Remote Learning Protocols

- Sessions will only be delivered via approved platforms.
- Parents/carers will be notified in advance and must give consent.
- Children must never be left unsupervised in a virtual room.
- Staff will use organisational devices/accounts only.
- Sessions will not be recorded without parental/carer consent and prior approval.

Appendix D – Online Safety Incident Reporting Flowchart

1. Online safety concern identified
2. Reported immediately to DSL/OSL (Kim Webster-Marsh) or Deputy DSL
3. Concern logged on safeguarding concern form
4. DSL/OSL assesses concern:
    - **Low level** → Record and monitor
    - **Emerging** → Discuss with parents/carers unless risk is posed
    - **Serious** → Refer to LADO, Police, or Suffolk MASH
5. Actions recorded and reviewed

Appendix E – Staff Online Safety Training Log

| Staff Name | Job Title | Start Date | Induction Training Date | Online Safety Modules Completed (e.g., Prevent, Cyberbullying, SEND-Specific Risks, AI Risks) | Provider | Latest Refresher Date | Next Due | Notes |

Appendix F – Acceptable Use Summary (Staff & Children)

- **Staff:** Must not use personal devices for child interaction, must model safe online behaviour, and must report incidents immediately.
- **Children:** Only use approved devices/platforms with supervision. No unsupervised messaging, gaming, or content searching.
- **Parents/Carers:** Informed about children's online activity in provision and provided with advice to support online safety at home.