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 - 

Data Protection and GDPR Policy

Building SEND Castles Ltd

1. Policy Statement

Building SEND Castles Ltd is committed to ensuring that personal information is handled lawfully, transparently, and securely, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
This policy outlines our approach to the collection, use, storage, and protection of data, with particular care given to sensitive information relating to children with Special Educational Needs (SEN), Speech, Language and Communication Needs (SLCN), their families, and staff. All data processing is conducted in a way that supports safeguarding and child protection, in line with KCSIE 2025 and Working Together to Safeguard Children (2023).

2. Scope

This policy applies to all staff, volunteers, contractors, and any individual who has access to personal or sensitive data within our organisation. It covers data relating to:

- Children and families
- Staff and volunteers
- Professional partners and agencies

3. Legal Framework

We comply with the following key legislation:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000 (where applicable)
- Children Act 1989 & 2004
- Working Together to Safeguard Children (2023)
- Keeping Children Safe in Education (KCSIE 2025)

4. Data Principles

We adhere to the following principles. Data must be:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept only for as long as necessary
- Processed securely to protect against unauthorised or unlawful use, loss, or disclosure

5. Lawful Bases for Processing

We process data on one or more of the following lawful bases:

- Legal obligation (e.g., safeguarding, statutory reporting)
- Vital interests (e.g., emergency medical care)
- Legitimate interests (e.g., service improvement, operational planning)
- Consent (e.g., photographs, newsletters)
- Public task (e.g., provision of education and care)

Where consent is used, it is obtained freely, clearly, and can be withdrawn at any time.

6. Data Collected

We may collect the following types of personal and sensitive data:

- Names, addresses, dates of birth
- Emergency contacts
- Medical information, SEN needs, care plans
- Educational reports, EHCPs, behaviour records
- Safeguarding and incident reports
- Employment and volunteer data (e.g., DBS checks, training records)

All data collection is proportionate to safeguarding and educational needs.

7. Data Storage and Security

- Paper records are stored in locked cabinets in a secure office
- Digital data is stored on encrypted, password-protected systems
- Access is limited to authorised personnel only
- Devices are protected by anti-virus software and regular backups
- We use secure methods for data transfer (e.g., secure email, encrypted files)
- All data handling complies with safeguarding, online safety, and KCSIE 2025 requirements

7a. Handling Information Received from External Agencies (including SCC and Schools)

- All information received from Suffolk County Council (SCC) or other external agencies is securely logged and transferred into our electronic child records/case management system immediately upon receipt.

- Original correspondence is stored temporarily in a secure location until the transfer is confirmed. Once transferred, any originals that are no longer required are securely destroyed.

- Electronic records are stored in password-protected, access-controlled systems, with all actions and updates logged.

- Information is retained according to statutory safeguarding requirements and our retention schedule (see Section 9).

7b. Data Destruction at the End of Retention Period

- All electronic and paper records are securely destroyed at the end of the retention period.

- Electronic files are permanently deleted using secure deletion software.

- Paper records are shredded using a cross-cut shredder.

- Destruction is logged internally, and a destruction certificate can be provided if required.

8. Data Sharing

We may share data with the following, where lawful and necessary:

- Suffolk County Council (e.g., safeguarding, SEN support)

- Health professionals and educational psychologists

- Social workers and Early Help teams

- Local Authority Designated Officer (LADO) and police where appropriate

- Parents/carers (in line with child's rights and age)

We never sell personal data or share it without a clear, lawful purpose.

9. Data Retention

- Records are retained according to statutory guidance (e.g., 25 years for safeguarding concerns) and securely destroyed when no longer required.
- A full retention schedule is available on request.
- All information received from SCC or outside agencies is also processed in line with our Safeguarding Policy to ensure any child protection concerns are acted upon promptly.

10. Subject Access Requests

Parents/carers, staff, or individuals over 13 have the right to:

- Request a copy of their personal data
- Request corrections to inaccurate data
- Request deletion of data (where lawful)
- Object to data processing

Requests will be responded to within one calendar month. Identity verification is required before release.

11. Breach Notification

- Any data breach will be logged and investigated.
- If a breach poses a risk to individual rights, the ICO will be informed within 72 hours and affected parties notified.
- All breaches involving safeguarding data will be escalated to the DSL and CEO immediately.

12. Staff Responsibilities and Training

- All staff must complete ICO-approved data protection training videos as part of induction and refresher training. This ensures consistent awareness of data protection duties and practical compliance.

- All staff must follow this policy and attend annual Data Protection and Confidentiality training.

- Staff must report concerns or breaches immediately to the CEO/Data Protection Lead.

- Confidential conversations should be held in private spaces, and records handled sensitively.

- Data protection forms part of safeguarding training and online safety practices for all staff.

13. Data Protection Officer (DPO)

Building SEND Castles Ltd is registered with the Information Commissioner's Office (ICO). The CEO, Kim Webster-Marsh, acts as the DPO and has completed accredited Data Protection Officer training.
She is responsible for compliance, training, and responding to access requests.

- Email: buildingsendcastles@gmail.com

- Phone: 07879793763

14. Policy Review

This policy will be reviewed annually or in response to legal changes, breaches, or updated guidance.

Relationship to Other Policies

This Data Protection Policy works in conjunction with the following organisational policies to ensure consistent safeguarding and operational compliance:

- **Safeguarding Policy** – Personal and sensitive data, including information received from Suffolk County Council (SCC), is used to support safeguarding procedures and child protection actions. All data handling aligns with the principles and responsibilities outlined in the Safeguarding Policy.

- **Online Safety Policy** – Data protection principles are applied to online platforms, devices, and digital communications, ensuring children, staff, and volunteers are safeguarded during technology use. Staff training in both areas is integrated.

- **Health and Safety Policy** – Incident reporting and record-keeping are conducted securely and in line with both health and safety and data protection requirements. This ensures any accidents, injuries, or near-misses are logged appropriately without compromising personal data.

- **Missing Children Policy** – Any records or reports generated when a child is missing are processed and stored securely, in line with statutory retention requirements and GDPR principles.

- **Allegations Against Staff Policy** – Allegations and investigation records are treated as sensitive personal data, stored securely, and retained or destroyed according to statutory guidance.

By cross-referencing these policies, Building SEND Castles Ltd ensures that data protection underpins all safeguarding, safety, and operational procedures, promoting a consistent and legally compliant approach across the organisation.