Data Practices

Overview

We believe in collecting as little data as possible. This document explains what we collect for both Storytailor (our web platform) and Story Intelligence™ (our future AI engine), why we need it, and how long we keep it.

Both products share the same data practices and retention policies, ensuring consistent privacy protection.

Data Collection

What We Collect

Here's everything we collect:

For All Users: - Age (we need this to know if COPPA protections apply, and to create age-appropriate stories) - Email address (for account access and communication)

For Children Under 13 (Current - Storytailor 3.0): - Parent email address (required by COPPA so we can get parental consent) - Stories they create (so they can save and return to their stories) - Character traits and preferences (to make stories feel personal)

Additional Data When Story Intelligence™ is Integrated (Future - Storytailor 4.0): - Voice conversations (these help create stories through talking, and we delete them after 30 days) - Emotional state information (helps us understand what kind of story a child needs, and supports safety monitoring)

For Parents: - Parent email address (for communication and consent management) - Information provided when giving consent for child's account

What Data We Do NOT Collect

Storytailor does NOT collect: - Full names - Physical addresses - Phone numbers - School information - Photos or videos - Location data (beyond IP address for security purposes) - Social media information - Payment information (handled by third-party payment processors)

Why We Collect Data

Purpose-Based Collection

Storytailor only collects data for the following purposes:

1. Service Delivery - Story generation and creation - Character management - Conversation continuity - User account management

2. Safety and Security - Safety incident detection - Crisis intervention - Parent notifications - Security monitoring

3. Compliance - Age verification (COPPA requirement) - Parental consent management (COPPA requirement) - Legal compliance and audit requirements

4. Service Improvement - Anonymized emotional data analysis (after 1 year retention period) - Service quality improvement - User experience enhancement

We never sell data to third parties. We never use data for advertising or marketing purposes.

How We Use Data

Story Generation (Current - Storytailor 3.0)

Stories and Characters: - Used to save stories children create - Used to maintain character consistency across stories - Stored until user deletes them

Character Preferences: - Used to create characters that match child's interests - Stored until user deletes character

Additional Features (Future - Story Intelligence™)

Voice Conversations: - Will be used to understand child's interests through talking - Will help generate age-appropriate stories through conversation - Will be retained for 30 days, then permanently deleted

Emotional State Data: - Will be used to understand child's emotional needs - Will be used for therapeutic story pathways - Will be used for safety monitoring - Will be retained for 365 days, then anonymized (personal identifiers removed)

Safety and Security

Safety Incident Detection (Both Products): - Content monitored for concerning material - Safety incidents trigger parent notifications - Incident summaries stored (content hashed, not raw text) - Retained for 7 years (legal requirement), then anonymized

Enhanced Safety (Story Intelligence™ - Future): - Voice conversations will be analyzed for concerning content - Real-time crisis detection and intervention - Advanced emotional state monitoring

Security Monitoring (Both Products): - IP addresses logged for security purposes - Authentication events logged - Security violations logged - Used for fraud prevention and

security incident response

Compliance

Age Verification: - Age used to determine COPPA protection status - Age used for age-appropriate content generation - Stored as part of user account

Parental Consent: - Parent email used for consent requests and notifications - Consent status tracked and logged - Consent history maintained for audit purposes

Data Retention Policies

Automated Retention Periods

Storytailor implements automated data retention and deletion:

Data Type	Retention Period	What Happens After
Voice Conversation Transcripts	30 days	Permanently deleted
Emotional State Data	365 days	Anonymized (personal identifiers removed)
Conversation States	24 hours	Permanently deleted
Voice Codes	1 day	Permanently deleted
Stories	Until deleted by user	User-controlled deletion
Characters	Until deleted by user	User-controlled deletion
Audit Logs	7 years	Anonymized (legal requirement)
Safety Incident Records	7 years	Anonymized after 1 year
Parent Email	Until account deleted	Deleted with account

Automated Deletion Process

How It Works: 1. System automatically identifies data that has exceeded retention period 2. Data is permanently deleted or anonymized based on deletion strategy 3. Deletion is logged for audit purposes 4. No manual intervention required

Deletion Strategies: - **Hard Delete:** Data is permanently removed and cannot be recovered - **Anonymization:** Personal identifiers are removed, but anonymized data may be retained for service improvement

Manual Deletion

Parent-Requested Deletion: - Parents can request immediate deletion of all child data - Deletion occurs immediately upon verified request - All child data is permanently deleted - Audit logs are anonymized (retained for legal compliance) - Parent receives confirmation of deletion

User-Controlled Deletion: - Users can delete their own stories and characters at any time - Deletion is immediate and permanent - No recovery possible after deletion

Account Deletion: - Account deletion removes all associated data - All user data, stories, characters, and preferences are deleted - Audit logs are anonymized - Parent email is deleted

Data Minimization for Children

Enhanced Protections for COPPA-Protected Users

Children under 13 receive enhanced data protection:

Stricter Retention: - Shorter retention periods where possible - Faster anonymization of emotional data - Enhanced deletion processes

Content Protection: - Safety incident content is hashed (not stored as raw text) - Only incident summaries stored - Enhanced privacy protections

Access Restrictions: - Stricter access controls - Enhanced audit logging - Parent-only data access

Data Sharing

Third-Party Services

Storytailor uses third-party services to provide the platform:

AWS (Amazon Web Services): - **Purpose:** Infrastructure and storage - **Data Shared:** Stories, characters, account information - **Protection:** Encryption at rest and in transit, Data Processing Agreement (DPA)

Supabase: - **Purpose:** Database storage - **Data Shared:** All user data stored in database - **Protection:** Encryption, Row Level Security, DPA available

SendGrid (Twilio): - **Purpose:** Email delivery to parents - **Data Shared:** Only parent email addresses (not child data) - **Protection:** TLS encryption, HIPAA-compliant options available

Data Processing Agreements: - All third-party services have Data Processing Agreements (DPAs) - DPAs ensure services only use data to provide the service - DPAs require appropriate security measures - DPAs require compliance with applicable privacy laws

No Data Sales: - Storytailor never sells data to third parties - Storytailor never shares data for marketing or advertising - Data is only shared with service providers necessary for platform operation

Data Security

Encryption

At Rest: - All data encrypted when stored - Database-level encryption enabled - Encryption keys managed securely

In Transit: - All API communications use TLS 1.3 - HTTPS required for all endpoints - Email delivery uses TLS encryption

Access Control

Row Level Security: - Database tables protected by Row Level Security (RLS) - Users can only access their own data - Parents can only access their own child's data - Service access restricted to system operations

Authentication: - All API endpoints require authentication - JWT Bearer tokens for authentication - Token validation on every request - Parent-child relationship verification

Data Export

Parent Data Export Rights

Parents can request export of all child data:

Export Contents: - User profile information - All story content - All character data - All emotional state data - Consent records - Safety incident summaries

Export Format: - Machine-readable format (JSON) - Downloadable from secure link - Link expires after 7 days - Includes all data types collected

How to Request: - Email: privacy@storytailor.com - Include parent name, relationship to child, child's user ID or email - Verification of parent identity required

Contact Information

Privacy Inquiries: privacy@storytailor.com
Technical Contact: tech@storytailor.com
Mailing Address:
Storytailor Inc.

7131 w 135th, #1074
Overland Park, KS 66223

Response Time: All privacy inquiries responded to within 30 days.

Storytailor Inc.
7131 w 135th, #1074
Overland Park, KS 66223