COPPA Compliance Documentation

Overview

COPPA compliance is central to both Storytailor (our web platform at Storytailor.com) and Story Intelligence™ (our AI engine for future versions and partner licensing). This document walks through our compliance measures and explains how we've implemented each requirement from COPPA regulations (16 CFR Part 312, sections §312.2-312.6).

Both systems share the same COPPA infrastructure, ensuring consistent protection whether children use Storytailor 3.0 today or Storytailor 4.0 with Story Intelligence™ in the future.

Age Threshold Protection

Automatic COPPA Protection

When a child under 13 tries to register, COPPA protections kick in automatically. We've built this protection into the database itself—not just the application code—so there's no way to bypass it:

At the Database Level: - Registration fails if a child under 13 doesn't have a parent email address - This happens at the database layer, before any application code runs - It's technically impossible to create an account for a child without parental information

At the Application Level: - Every child under 13 gets automatically flagged for COPPA protection - The system checks this flag before collecting any data - Parent consent must be verified before the child can use the service

Age Verification Process

During Registration: 1. The child enters their age 2. If they're under 13, we immediately require a parent email address 3. No parent email? Registration stops with a clear explanation 4. With parent email? Account is created with COPPA protections enabled

After Registration: - We check COPPA protection status with every request - We won't collect data until parental consent is verified - All data operations respect these protections

Verifiable Parental Consent (VPC)

COPPA §312.2 - Verifiable Parental Consent

Storytailor implements a Verifiable Parental Consent (VPC) workflow that complies with COPPA requirements.

Consent Request Process

The same consent process applies to both Storytailor 3.0 and Story Intelligence™ :

Step 1: Consent Request Creation - When a child under 13 registers, a consent request is automatically created - Parent email address is validated - Unique consent request ID is generated - Consent request is stored with status “pending” - Consent request expires after 7 days if not verified

Step 2: Parent Notification - Parent receives email notification explaining: - What Storytailor does (current features in 3.0) - What Story Intelligence™ will add in the future (voice, emotion detection) - Exactly what data will be collected - Instructions for providing consent

Step 3: Consent Verification - Parent can verify consent through email link - Consent verification requires validation of request ID - Upon verification, consent status is updated to “verified” - Consent timestamp is recorded for audit purposes

Step 4: Consent Status Tracking - System maintains current consent status for each child - Consent status can be checked at any time - Consent history is maintained for audit purposes

Consent Revocation

Parents can revoke consent at any time: - Revocation immediately stops all data collection - Existing data can be deleted upon parent request - Revocation is logged and timestamped - Parent receives confirmation of revocation

Consent Status Values

- **none:** No consent request has been created
- **pending:** Consent request created, awaiting parent verification
- **verified:** Parent has verified consent, data collection permitted
- **revoked:** Parent has revoked consent, data collection stopped

Notice Requirements

COPPA §312.3 - Notice to Parents

Storytailor provides comprehensive notice to parents through:

Privacy Policy: - Child-friendly privacy policy written in simple language - Clear explanation of data collection practices - Detailed description of how data is used - Parental rights explanation - Data retention policies - Third-party service disclosure

Direct Notice: - Email notification to parent when consent is requested - Email includes link to privacy policy - Email explains what data will be collected and why - Email provides instructions for providing or denying consent

Data Minimization

COPPA §312.4 - Data Minimization

Storytailor follows strict data minimization principles:

Purpose-Based Collection: - Only data necessary for service delivery is collected - No data is collected for marketing or advertising purposes - No data is sold to third parties

Minimal Data Collection: - User age (required for COPPA compliance) - Parent email address (required for users under 13) - Voice conversation transcripts (30-day retention) - Story content created by users - Character preferences and traits - Emotional state data (365-day retention, then anonymized)

What We Do NOT Collect: - Full names - Physical addresses - Phone numbers - School information - Photos or videos - Location data (beyond IP address for security)

Parental Rights

COPPA §312.5 - Parental Rights

Storytailor provides comprehensive parental rights:

Right to Access

Parents can request access to all information collected about their child: - Request can be made via email or API - Information is provided within 30 days - Information includes: user data, stories, characters, emotions, consent records, safety incidents - Information is provided in machine-readable format (JSON)

Right to Delete

Parents can request deletion of all child data: - Request can be made via email or API - 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

Right to Export

Parents can request export of all child data: - Request can be made via email or API - Data is provided in JSON format - Downloadable from secure link (expires in 7 days) - Includes all data types collected

Right to Revoke Consent

Parents can revoke consent at any time: - Revocation can be made via email or API - Revocation immediately stops data collection - Existing data can be deleted upon request - Parent receives confirmation of revocation

How Parents Exercise Rights

Via Email: - Send email to privacy@storytailor.com - Include parent name, relationship to child, child's user ID or email - Specify type of request (access, deletion, export, revoke consent) - Include verification of parent identity

Via API: - Use REST API endpoints with parent authentication - All requests are logged for audit purposes - Responses provided in JSON format

Data Retention and Deletion

Automated Data Retention Policies

Storytailor implements automated data retention and deletion:

Data Type	Retention Period	Deletion Strategy
Voice Transcripts	30 days	Hard delete
Emotional Data	365 days	Anonymize
Conversation States	24 hours	Hard delete
Voice Codes	1 day	Hard delete
Audit Logs	7 years	Anonymize (legal requirement)
Stories	Until deleted by user	User-controlled
Characters	Until deleted by user	User-controlled

Automated Deletion: - Data is automatically deleted when retention period expires - No manual intervention required - Deletion is logged for audit purposes

Manual Deletion: - Parents can request immediate deletion at any time - Users can delete their own stories and characters - Account deletion removes all associated data

Security Measures

Encryption

Encryption at Rest: - All data stored in encrypted databases - Encryption keys managed securely - Database-level encryption enabled

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

Access Control

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

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

Audit Logging

Logged Events: - User authentication - Consent requests and verifications - Consent revocations - Data access requests - Data deletion requests - Safety incidents - API errors and security violations

Audit Log Retention: - Audit logs retained for 7 years (legal requirement) - Logs anonymized after 1 year for privacy - Logs used for compliance verification and security monitoring

Compliance Verification

Testing and Verification

Storytailor has implemented comprehensive testing to verify COPPA compliance:

Age Verification Testing: - Tested user registration with various ages - Verified COPPA protection applies to users under 13 - Verified parent email requirement enforcement - Confirmed registration rejection when parent email missing

Consent Workflow Testing: - Tested complete consent request → verification → status check workflow - Verified consent expiration after 7 days - Tested consent revocation process - Confirmed consent status tracking

Parental Rights Testing: - Tested data access endpoint - Tested data deletion endpoint - Tested data export endpoint - Verified all requests are logged

Compliance Monitoring

Ongoing Monitoring: - Regular review of consent status - Monitoring of data retention compliance - Review of parental rights requests - Security incident monitoring - Audit log review

Compliance Reporting: - Consent status reports - Data retention compliance reports - Parental rights request summaries - Security incident summaries

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